EQSC

eqscglobal.com

Data-Driven Clarity
For Higher Education Leaders.

Academic Analytics | Executive Intelligence

EQSC

eqscglobal.com

University Digital Resilience

Systems, Suppliers and Recovery Capability

Global evidence with regional analysis of the United Kingdom, the Gulf (GCC) and India

EQSC

eqscglobal.com/ready-reports

University Digital Resilience

Systems, Suppliers and Recovery Capability

(Global evidence with regional analysis of the United Kingdom, the Gulf (GCC) and India)

Research Production Notice

The report compiles attributed public evidence, editorial calculations and a separate synthetic demonstration dataset. The modelled results are not observed institutional outcomes, and no primary survey of the 240 synthetic institutions was undertaken. This publication does not certify any named institution or constitute legal, financial, technical-audit or regulatory advice.

Disclaimer and Publication Notice

All third-party images, data, figures, and institutional references within this report are utilized strictly for non-commercial educational and research purposes under applicable "fair use" exceptions. Full authorship, title, and intellectual property rights remain exclusively with their respective legal owners.

EQSC Global explicitly disclaims any and all liability, responsibility, or warranties - express or implied - regarding the accuracy, completeness, interpretation, reproduction, or subsequent use of these third-party materials to the maximum extent permitted by law.

This document serves as a public evidence review synthesizing secondary data (including official labor statistics, academic research, and employer studies), not a primary survey. Third-party findings are attributed to their original publishers, and any subsequent publication, reproduction, or commercial resale of the underlying manuscript or figures requires independent verification and explicit clearance from the rightful copyright holders.

About EQSC Global

EQSC Global is presented in this publication as an international research, analytics and consultancy organisation. This report addresses university leaders, researchers, sector bodies and professional decision-makers interested in the resilience of essential digital services.

Editorial context

The central question is not whether a university can prevent every cyber incident. It is whether the institution knows which services matter most, understands the suppliers on which they depend and can restore those services within a workable timeframe. The analysis draws on public sources published through early October 2026 and distinguishes direct published evidence from calculated indicators, analyst interpretation and synthetic exercises.

About this report and how to read the evidence

This report examines the ability of universities to maintain essential digital services, respond to supplier-originated incidents and restore operations after disruption. It brings together international evidence and more detailed material from the United Kingdom, the Gulf Cooperation Council (GCC), particularly the UAE, Saudi Arabia and Qatar, and India. The analysis focuses on what institutions can measure and improve, rather than treating cyber security as a purely technical compliance question.

Data provenance statement (please read before citing)

- This is a model report with two layers of data, always kept apart. (1) Published evidence: the statistics in Sections 1–11 are attributed to named public sources; selective external checks do not constitute verification of every claim and referenced in square brackets, e.g. [1], which maps to the numbered reference list. (2) Modelled data: Section 12 presents a synthetic benchmark dataset (240 institutions) built to sit close to real-world figures and to show what the primary study would produce.
- Modelled data are labelled everywhere they appear. Each modelled chart carries a red "MODELLED DATA - ILLUSTRATIVE" stamp, and each modelled table or paragraph is marked as such. Modelled values describe no real institution and must not be quoted as observed statistics.
- Derived indicators are labelled as such. Where this report calculates something new (e.g., the Control Coverage Index, gap ratios, a partial Herfindahl–Hirschman Index), the derived-index calculations use published inputs, the method is shown, and the result is marked "author calculation".
- Primary data are not yet collected. The proposed survey, authorised incident and recovery records, and the non-intrusive control and tabletop review require institutional consent. The modelled dataset (Section 12) and the ready-to-field toolkit (Annexes A–D) show exactly how that evidence would be gathered and analysed.
- Comparability caveats are stated where they matter. Vendor surveys, telemetry and official statistics use different definitions, samples and periods; the report does not average them together.

Scope and intended use

This edition is a public, secondary-evidence research report with one separately labelled synthetic benchmark section. Its measures and research instruments may inform institutional planning, but the report is not a certification, audit or assessment of named universities. Any institution-specific findings would require authorisation and new data collection.

Evidence grading used throughout

Grade	Source type	Examples used in this report
A	Official statistics and statutory/government publications	UK Cyber Security Breaches Survey (accredited official statistics); HESA; AISHE; CERT-In / PIB releases; Gazette-notified rules
B	Regulators, national CERTs/cyber agencies, sector bodies, institutional disclosures	NCSC Annual Review; Jisc; British Library incident review; university incident pages; UAE Cyber Security Council; Saudi NCA
C	Independent or vendor-commissioned surveys with disclosed methods	Sophos State of Ransomware series; IBM Cost of a Data Breach; Verizon DBIR; KnowBe4 benchmarking
D	Vendor telemetry and quality media reporting of incidents	Check Point Research weekly-attack telemetry; Positive Technologies; trade-press incident reports

Evidence grades indicate the provenance and transparency of a source, rather than the importance of the issue it describes. Official data and institutional disclosures carry different kinds of weight from commercial surveys and vendor telemetry; the latter are useful signals, but should not be read as representative population estimates.

Research questions and scope

1. **Readiness:** How prepared are universities for service disruptions and supplier incidents (planning, controls, supplier governance)?
2. **Recovery capability:** How quickly and how completely do institutions recover, and what determines the difference?
3. **Staff awareness:** What is the coverage and effectiveness of training and testing, and how does the human factor show up in incidents?
4. **Technology dependencies:** Where are universities concentrated on a small number of platforms and suppliers, and what happens when those fail?
5. **Response resources:** What people, money, insurance, external support and regulation are available to respond?

The report uses five measures consistently: time to recovery, control coverage, supplier concentration, training uptake and service exposure. Section 3 defines each measure, explains the calculation and identifies where direct institutional records would be needed to move beyond public proxies.

Contents

About this report and how to read the evidence 3
1. Executive summary 6
2. Global context: why universities are a uniquely exposed sector 9
3. Measurement framework: five resilience metrics 12
4. United Kingdom: deep dive 14
5. Control coverage analysis (derived index) 19
6. The Gulf (GCC): deep dive 21
7. India: deep dive 23
8. Technology dependencies and supplier concentration 25
9. Recovery capability 28
10. Staff awareness and response resources 30
11. Cross-regional comparison 32
12. Modelled benchmark study (illustrative) 34
13. Recommendations and roadmap 41
14. Tabletop exercise toolkit 43
Annex A. Primary survey instrument 44
Annex B. Authorised incident and recovery records protocol 46
Annex C. Non-intrusive control review checklist 47
Annex D. Ethics, legal and data-licensing notes 48
Glossary 49
Research limitations and interpretation 50
References 51
Commissioned consultancy reports 55

1. Executive summary

Universities depend on a complicated network of systems that must remain available through teaching, research, admissions and examinations. Many of these services now sit outside the institution itself, in shared learning platforms, hosted student records, identity services and specialist suppliers. That dependence has improved some aspects of security, but it has also made a single supplier failure capable of disrupting many campuses at once. Drawing on public statistics, sector incident records and a separately identified illustrative model, this report examines the gap between having controls on paper and being able to recover when those controls are tested.

Ten numbers that define the problem

- **98%** of UK higher education institutions identified a breach or attack in the last 12 months, against 43% of UK businesses (CSBS 2025/26) [1].
- **4,368** average weekly attacks per education organisation globally, the most of any sector; **8,487** per education organisation in India, 1.94x the global education figure (Check Point Research, 2025) [29].
- **8,809** institutions worldwide were affected by the April–May 2026 compromise of Instructure (Canvas LMS), one of the largest supplier incidents the sector has seen [12][11].
- **~890** US colleges and universities had data stolen through one intermediary (National Student Clearinghouse) in the 2023 MOVEit campaign [13].
- **80% vs 37%:** UK HE institutions reviewing risks in immediate suppliers vs the wider supply chain, a 43-point blind spot [1].
- **47%:** share of higher education ransomware victims that restored encrypted data from backups in 2025, down from 78% a year earlier (Sophos) [21][22].
- **95% / 71%:** share of attacked education organisations whose backups attackers tried to compromise, and the success rate of those attempts (Sophos 2024) [22].
- **6 hours** to report a cyber incident to CERT-In in India [33], compared with 72 hours for a personal-data breach under India's DPDP Rules [34] and under UK GDPR.
- **144,000+** compromised UK education and research username/password pairs found by Jisc in the 12 months to June 2026, a three-fold rise [4].
- **37%** of UK further education colleges have dedicated cyber security staff, compared with 92% of HE providers (Jisc) [3].

Key findings

Finding 1: Planning has caught up; supplier governance has not

The UK evidence points to a clear imbalance. Formal incident response plans increased from 75% to 92% between the 2025 and 2025/26 surveys; threat-intelligence use rose from 72% to 92%, and penetration testing from 69% to 84% [1][2]. Yet only 37% of surveyed higher education institutions reviewed risks beyond their immediate suppliers. The derived Control Coverage Index (Section 5) places supplier assurance at 58.5, well behind preparation (87.5) and protection (90.5). Strong internal arrangements, in other words, do not guarantee visibility across a shared service chain.

Finding 2: Supplier concentration has turned single incidents into sector-wide events

Several incidents show why concentration deserves board attention. The 2026 Canvas LMS breach affected institutions internationally; one secondary account reports 8,809 institutions, while the exact number requires direct confirmation [11][12]. The 2025 Oracle E-Business Suite exploitation, the

MOVEit campaign involving the National Student Clearinghouse, and the July 2024 CrowdStrike update failure likewise exposed the consequences of relying on common software, support processes or infrastructure [13][14][18]. These were not identical events, but each illustrates how risk can travel quickly across institutional boundaries. The three largest cloud infrastructure providers held a combined 63% market share in Q2 2026 [19]; a separate claim of approximately 70% UK higher education use for one student-records product remains secondary-source evidence [20].

Finding 3: Recovery is getting faster across the economy, but higher education lags on clean restoration

Ransomware victims across industries appear to be recovering more quickly: in the cited 2025 study, 53% reported full recovery within a week, compared with 35% in the previous wave [23]. UK and UAE cross-sector figures were 59% and 63%, respectively [23][24]. The education-specific evidence is more troubling. Higher education incidents resulted in encryption in 58% of cases, while only 47% of affected higher education respondents reported restoring encrypted data from backups [21]. The British Library's published incident review provides a practical reminder that rebuilding important services can continue long after an attacker has been contained [7].

Finding 4: Training reach is high, but awareness testing is uneven and credentials are the soft spot

Training is widely offered, but reach and effectiveness are different things. In the UK, more than nine in ten FE and HE institutions delivered cyber training [1], while the share of HE institutions reporting staff-awareness testing fell from 94% to 71% between survey waves [1][2]. Jisc also identified more than 144,000 compromised education and research credential pairs in the 12 months to June 2026 [4]. Repeated testing, reporting behaviour and privileged-user readiness therefore deserve as much attention as course-completion rates.

Finding 5: Regional readiness diverges sharply, and so does the evidence

- United Kingdom: The strongest institution-level evidence base of the three focus regions comes from official education surveys, Jisc telemetry and national incident reporting. Financial pressure still matters: 36% of English providers recorded a deficit in 2024/25, and more than 40% forecast deficits for 2025/26 [50].
- Gulf (GCC): National cyber frameworks are well established in several states, but published university-level recovery and control data are scarce. Saudi Arabia's ECC-2:2024 includes controls for third-party and cloud risk [42]. Dubai's international branch campuses introduce an additional dependency on parent institutions and their systems overseas [45].
- India: Check Point telemetry reports 8,487 weekly attack attempts per education organisation in the cited 2025 period [29]. CERT-In rules require reporting of specified incidents within six hours [33]. A large affiliated-college network and limited public information on institutional recovery make consistent measurement particularly important [47][48]. Substantive DPDP Act obligations are scheduled to commence in stages, with core operational provisions due in May 2027 [34].

Modelled benchmark headlines (illustrative -see Section 12)

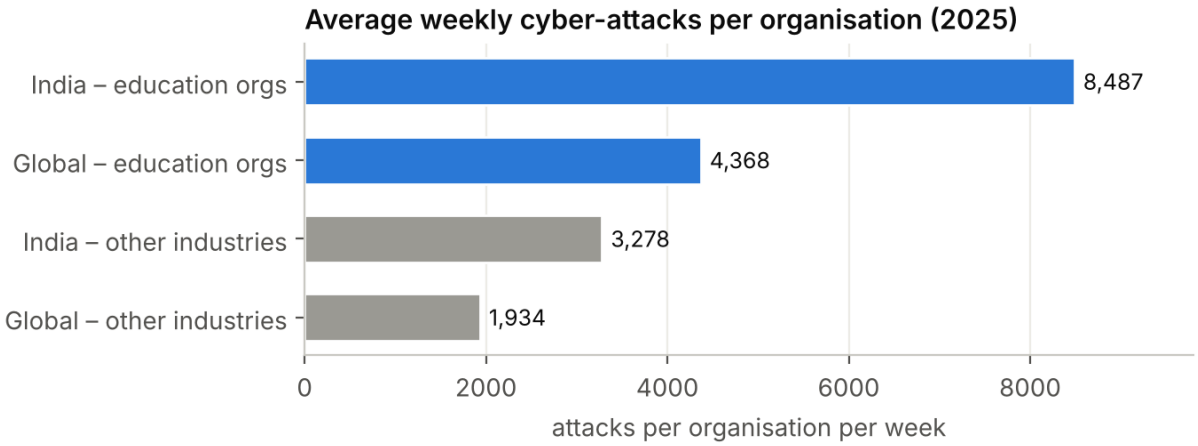
- **MODELLED DATA.** In a calibrated synthetic study of 240 institutions and 544 disruptive incidents, **supplier/platform failures were the most frequent cause of disruption** (173 incidents). Only 62% of them met the tier-1 recovery time objective.
- Modelled Control Coverage Index: **UK 65.4, Gulf 60.8, India 35.4** (16-control set). The widest gap within any region was between Indian private universities (53.8) and affiliated colleges (21.2).
- Modelled ransomware recovery with immutable backups took a median of **31.8 hours, against 87.0 hours** without them. A 24-hour supplier notification clause was associated with a **28% shorter** supplier-incident recovery.
- In 60 modelled tabletop exercises, the weakest criteria were **supplier engagement (1.27 of 3)** and **backup confidence (1.47 of 3)**.

2. Global context: why universities are a uniquely exposed sector

Higher education combines conditions rarely found together at this scale: open networks that support collaboration, a continually changing population of users, valuable research data, extensive personal records and considerable autonomy at departmental level. At the same time, admissions, examinations and results create periods when even a short interruption can be disproportionately costly. Universities have adopted shared software platforms widely; resilience increasingly depends on how well these dependencies are understood and governed.

2.1 Threat volume and targeting

Check Point Research telemetry placed education among the most heavily targeted sectors in its 2025 reporting, recording an average of 4,356 attempted weekly attacks per organisation from January to July 2025, 41% above the comparison period. Reported regional averages were 7,869 in Asia-Pacific, 4,473 in Africa, 4,161 in Europe, 3,164 in Latin America and 3,047 in North America [28]. In July 2025, the vendor also identified 18,391 newly registered education-related domains, roughly one in 57 of which it classified as malicious or suspicious [28]. These figures concern observed attempts and suspicious activity; they do not represent confirmed successful compromises.



Source: Check Point Research, as reported by CXO Digital Pulse, 22 Sep 2025. Telemetry-based; vendor-defined 'attack'.

Figure 1. Education organisations face more than twice the weekly attack volume of other industries, and Indian education organisations nearly double the global education average.

Vendor telemetry captures attempted and blocked activity rather than verified breaches. Figures also differ across reporting windows: Check Point reported 4,178 weekly attempts per education organisation in August 2025 [30] and 4,368 in the India-focused September release [29]. They indicate relative pressure on systems, not necessarily the number or severity of incidents experienced by universities.

2.2 How breaches actually happen

Table 1. Global breach patterns relevant to universities (Verizon DBIR 2025)

Indicator	Value	Relevance to universities
Confirmed breaches analysed	12,195 (of 22,052 incidents)	Largest annual breach dataset globally
Breaches involving a third party	30% (doubled from 15%)	Directly measures supplier-originated risk

Indicator	Value	Relevance to universities
Vulnerability exploitation as initial access	20%	Edge devices, VPNs, file-transfer and ERP platforms
Ransomware present in breaches	44% (up from 32%)	Main disruptive threat to teaching and research
Stolen credentials as initial vector	22%	Large, transient user populations; leaked student and staff logins
Victims not paying ransom	64% (up from 50%)	Recovery capability, not payment, is the main route back
Median ransom paid	US$115,000 (down from US$150,000)	Cross-sector benchmark

Source: Verizon 2025 Data Breach Investigations Report, as summarised by Help Net Security [26]. Grade C.

2.3 Ransomware in education: a fast-changing picture

The Sophos State of Ransomware in Education series provides one of the more consistent sets of cross-year observations on this issue, although it remains a survey rather than a census. The 2025 edition covered 441 education respondents in 17 countries and was conducted by Vanson Bourne [21][22]. Its results point to improvements in the frequency of encryption and reported recovery costs, alongside a serious deterioration in the proportion of higher education respondents able to restore encrypted data from backups.

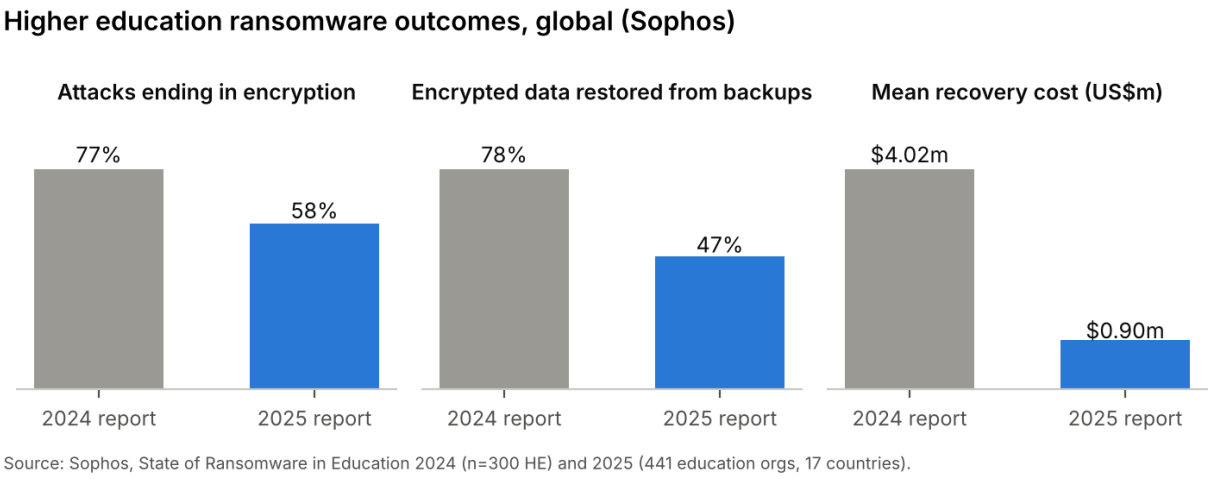


Figure 2. Fewer HE attacks ended in encryption and recovery costs fell, but the share of victims able to restore from backups fell sharply from 78% to 47%.

Table 2. Ransomware outcomes, lower vs higher education (Sophos 2025)

Measure	Lower education	Higher education
Attacks stopped before encryption	67% (from 14%)	38% (from 21%)
Attacks resulting in encryption	29%	58%
Median ransom demand	US$1.02m (from US$3.85m)	US$697k (from US$3.55m)
Median ransom payment	US$800k (from US$6.6m)	US$463k (from US$4.41m)
Mean recovery cost excl. ransom	US$2.20m (from US$3.76m)	US$0.90m (from US$4.02m)

Measure	Lower education	Higher education
Encrypted data restored via backups	59% (from 75%)	47% (from 78%)
Leading technical root cause	Phishing, 22%	Exploited vulnerabilities, 35%
Leading organisational factor	Lack of expertise / limited IR capacity, 42%	Unknown security gaps, 45–49%

Source: Sophos, The State of Ransomware in Education 2025 [21]; prior-year values from the 2024 edition [22]. Grade C.

The 2024 Sophos edition reported attempted backup compromise in 95% of ransomware incidents among education respondents, with attackers succeeding in 71% of those attempts [22]. The lesson for recovery planning is straightforward: a backup should not be assumed reliable merely because it exists. Isolation, separate administrative access and demonstrated restoration matter.

2.4 The human cost of incidents

The consequences extend beyond technology. In the 2025 Sophos education survey, substantial shares of affected IT and security personnel reported stress, anxiety, guilt or leave following an attack [21]. The British Library's review similarly identified staff and user wellbeing as a recovery lesson [7]. A prolonged incident can exhaust precisely the team on which an institution depends for restoration.

3. Measurement framework: five resilience metrics

A useful resilience assessment needs a small number of measures that can be applied consistently across institutions. The framework below translates the five research themes into operational definitions, sets out the available public proxies and identifies what an authorised primary study would need to collect. The survey instrument and records protocol in Annexes A and B use these same definitions.

Table 3. Metric definitions

Metric	Operational definition and formula	Best public proxy (2025–26)	Primary data required
Recovery time	Elapsed time from service loss to restoration of agreed minimum service, per tier-0 service. Report median and 90th percentile; compare against stated RTO. Recovery time ratio = actual ÷ RTO.	Share of ransomware victims fully recovered within one week (Sophos) [23][24]; incident case timelines [7][9][10]	Authorised incident logs with timestamps for detection, containment, minimum-service and full restoration
Control coverage	Share of a defined control set implemented and evidenced. Control Coverage Index (CCI) = unweighted mean of 14 indicator percentages, grouped into five pillars (Prepare, Protect, People, Suppliers, Recover).	UK CSBS indicator percentages [1]; Saudi ECC-2:2024 control count (108 controls) [42]	Non-intrusive evidence review against CAF/ECC/ISO 27001 control lists
Supplier concentration	Herfindahl–Hirschman Index (HHI) of tier-0 service hosting/provision: HHI = $\Sigma(s_i \times 100)^2$, where s_i is supplier share of tier-0 services. Plus "single-supplier critical paths" count.	Cloud market shares (top three = 63%) [19]; LMS/SIS market share disclosures [11][20]	Supplier register with service-to-supplier mapping, including fourth parties
Training uptake	Uptake = staff completing training in 12 months ÷ staff in scope. Effectiveness = phishing-simulation click rate, report rate and repeat-clicker rate.	CSBS training and awareness-testing rates [1]; KnowBe4 benchmarks [27]	LMS/HR completion data; phishing simulation platform exports
Service exposure	Exposure score per service = criticality (1–5) × external attack surface (1–5) × supplier dependency (1–5) × peak-period sensitivity (1–3). Max 375.	Internet-exposed asset counts (e.g., 223,800 exposed assets in the UAE) [39]; credential leaks [4]	Asset inventory, external attack-surface scan (authorised), business impact analysis

The measurement formulas and indicative service thresholds are proposed analytical tools within this report, not statutory or sector-wide standards. The Herfindahl–Hirschman Index (HHI) follows an established concentration formula; the service-specific implementation and other indices are illustrative analytical choices.

3.1 Control Coverage Index (CCI): method

To compare the breadth of controls reported by UK institution types, this report derives a Control Coverage Index (CCI) from the Cyber Security Breaches Survey 2025/26 education annex [1]. Fourteen distinct indicators are organised into five pillars. The index takes the unweighted average of the 14 adoption percentages; pillar scores are averages within each group. This is a measure of reported adoption, not direct confirmation that controls work during an incident.

Table 4. CCI indicator set and pillar mapping

Pillar	Indicators (CSBS 2025/26)
Prepare	Risk assessment covering cyber; threat intelligence; formal incident response plan; business continuity plan covering cyber
Protect	Multi-factor authentication; patching within 14 days; penetration testing; security monitoring tools
People	Training delivered; staff awareness testing (e.g., mock phishing)
Suppliers	Immediate supplier risk review; wider supply-chain risk review
Recover	Formal post-incident debrief; specific cyber insurance policy; business continuity plan covering cyber

BCP appears in two pillars by design (it is both a preparation and a recovery control); the overall CCI counts it once.

3.2 Recovery time tiers

Service tier	Typical university services	Suggested RTO / RPO benchmark
Tier 0: foundational	Identity & SSO, DNS, network core, endpoint management, backup platform	RTO ≤ 24 hours; RPO ≤ 1 hour
Tier 1: mission-critical	LMS/VLE, student records (SIS), email & collaboration, payroll, research data storage	RTO ≤ 72 hours; RPO ≤ 4 hours; peak-period RTO ≤ 24 hours
Tier 2: important	Finance/ERP, library platform, timetabling, CRM/admissions, HR	RTO ≤ 7 days; RPO ≤ 24 hours
Tier 3: deferrable	Departmental websites, archives, non-critical apps	RTO ≤ 30 days

These recovery time and recovery point objectives are proposed starting assumptions for institutional discussion, not mandatory benchmarks. Universities should replace them with targets grounded in their own business impact analyses, academic calendars, data retention needs and supplier contracts.

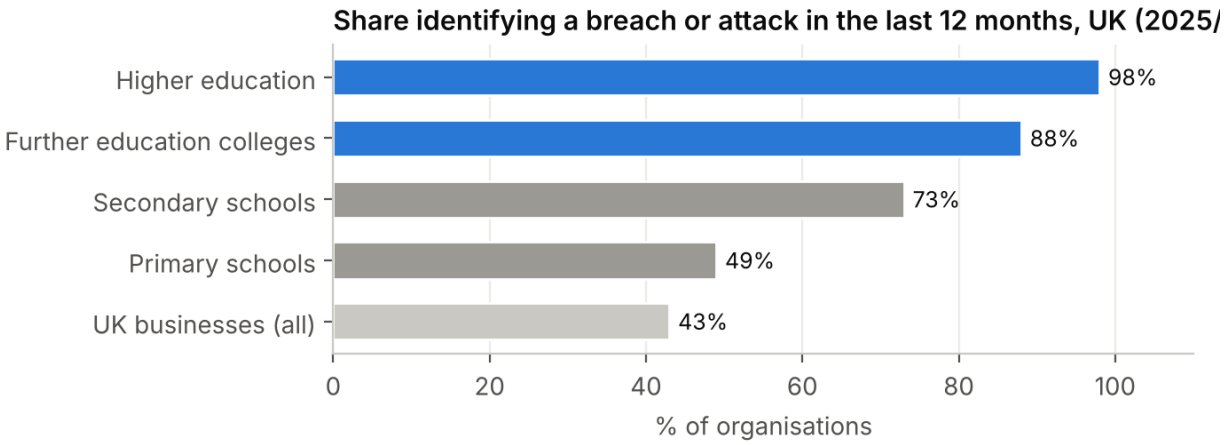
4. United Kingdom: deep dive

4.1 Sector profile

UK higher education enrolled **2,863,180** students in 2024/25, down 1% on 2023/24; about one in four students came from outside the UK, and India and China together accounted for 47% of non-EU international enrolment [49]. The sector is under financial pressure: the Office for Students reported that 36% of English providers were in deficit in 2024/25 and over 40% forecast deficits for 2025/26. In its most severe modelled scenario, around 200 providers (70% of the sector) would be in deficit by 2028/29 [50]. Resilience investment competes directly with these pressures.

4.2 Official statistics: the Cyber Security Breaches Survey

The UK Cyber Security Breaches Survey provides a repeated, probability-based measure of publicly funded education institutions, although it is not a technical audit. The 2025/26 edition surveyed 273 primary schools, 222 secondary schools, 33 further education (FE) colleges and 49 higher education (HE) institutions between August and December 2025 [1]. The relatively small FE and HE samples warrant care when comparing estimates or interpreting year-on-year changes.



Source: DSIT/Home Office, Cyber Security Breaches Survey 2025/26 – Education Institutions Findings (30 Apr 2026). HE n=49 (±11.9pp).

Figure 3. Almost every UK university identified a breach or attack in the past year, more than twice the rate among UK businesses.

Table 5. Attack types among UK institutions identifying breaches (CSBS 2025/26)

Attack type	Primary	Secondary	FE & HE	Businesses
Phishing	90%	96%	96%	88%
Impersonation	31%	44%	79%	28%
Viruses, spyware or malware	11%	15%	51%	16%
Denial of service	3%	7%	49%	6%
Ransomware	0%	6%	14%	3%
Unauthorised access by staff	2%	12%	29%	2%
Unauthorised access by students	1%	10%	23%	n/a
Any negative outcome (e.g., compromised accounts, service loss)	13%	20%	49%	19%

Source: CSBS 2025/26 Education Institutions Findings [1]. Grade A. FE and HE are reported combined for attack types.

Among FE and HE institutions with breaches, the most common negative outcomes were compromised accounts (23%), service slowdown or takedown (16%) and loss of access to files or networks (14%) [1]. **Insider and student unauthorised access (29% and 23%)** is a distinctive higher-education risk: institutions must defend against their own users as well as external attackers.

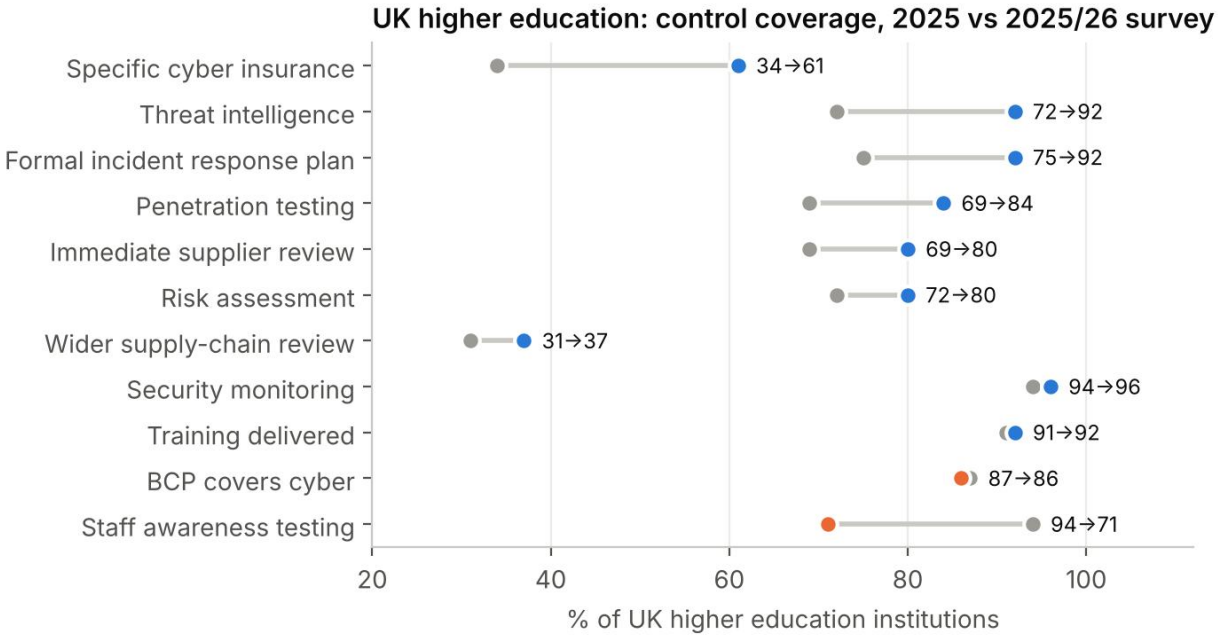
Table 6. Readiness controls by UK institution type (CSBS 2025/26)

Control	Primary	Secondary	FE	HE	Businesses
Board member responsible for cyber	85%	73%	82%	100%	31%
Governors updated quarterly or more	60%	64%	79%	84%	–
Risk assessment covering cyber	61%	64%	85%	80%	–
Security monitoring tools	51%	66%	79%	96%	–
Penetration testing	23%	38%	52%	84%	–
Threat intelligence	18%	32%	45%	92%	–
Formal incident response plan	73%	77%	79%	92%	25%
Post-incident debrief process	75%	85%	64%	84%	–
BCP covers cyber	74%	80%	79%	86%	33%
Multi-factor authentication	89%	86%	94%	98%	47%
Patching within 14 days	45%	62%	73%	84%	34%
Organisation-owned devices only	82%	58%	58%	20%	66%
All 10 Steps to Cyber Security covered	14%	23%	33%	45%	3%
Specific cyber insurance policy	9%	15%	36%	61%	–

Source: CSBS 2025/26 [1]. Grade A. "–" indicates the comparison was not reported in the source extract.

Two contrasts deserve attention. Only 20% of surveyed HE institutions reported restricting access to organisation-owned devices, compared with 66% of businesses overall [1]. That is consistent with the practical realities of students, staff and researchers using a variety of devices, and it increases the value of identity controls and monitoring. Meanwhile, 45% of HE institutions said they covered all ten of the NCSC's 10 Steps to Cyber Security, despite universal coverage of at least five steps [1].

4.3 What changed between survey waves

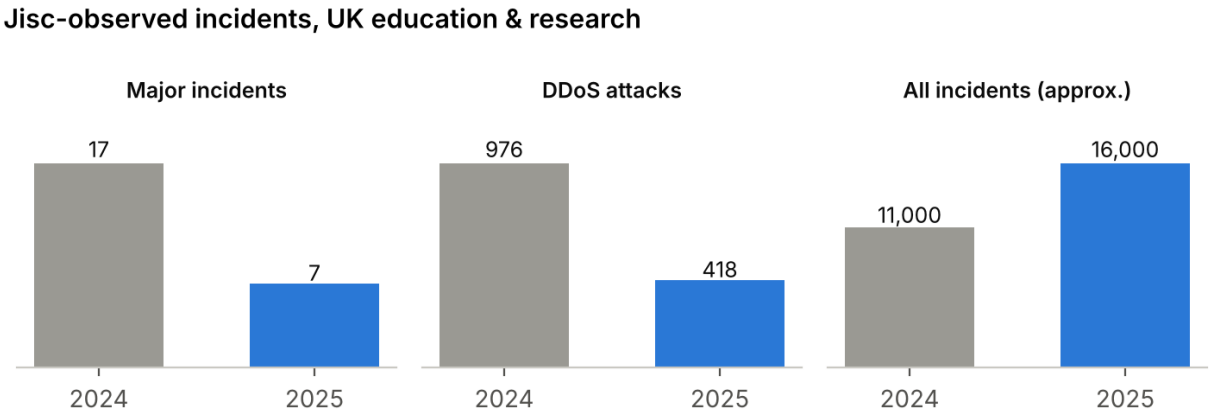


Source: CSBS 2025 (fieldwork Aug–Dec 2024, HE n=32) and CSBS 2025/26 (Aug–Dec 2025, HE n=49). Small samples: treat changes <12pp as indicative.

Figure 4. UK HE strengthened insurance, threat intelligence, incident response planning and testing; recorded staff-awareness testing fell.

Survey changes must be treated cautiously: HE respondent bases were 32 in the 2025 wave and 49 in 2025/26. Differences near the sampling error may not indicate a real shift. Larger reported changes nevertheless merit attention, including cyber insurance (+27 percentage points), threat intelligence (+20), incident response plans (+17) and penetration testing (+15). Staff-awareness testing moved in the opposite direction, from 94% to 71% [1][2].

4.4 Sector telemetry: Jisc and the NCSC



Source: Jisc news release on its Cyber Threat Intelligence Report ('over 11,000' and 'over 16,000' incidents).

Figure 5. Jisc recorded fewer major incidents and DDoS attacks in 2025, but more incidents overall, and warned that the remaining attacks are more sophisticated.

Jisc, which operates the Janet network and the sector CSIRT, recorded 7 major incidents in 2025 against 17 in 2024, and 418 DDoS attacks against 976, while the total number of incidents rose from over 11,000 to over 16,000. It reported evidence of state sponsorship and AI adoption by criminals, and named ransomware and phishing as the top threats for HE and FE [3]. Its posture survey found that 92% of HE providers but only 37% of FE colleges employ dedicated cyber security staff [3]. In the 12

months to June 2026, Jisc found more than 144,000 compromised username/password pairs for UK education and research identities, ranging from 3,500 in January 2026 to 26,300 in May 2026 [4].

At national level, the NCSC handled 429 incidents (from 1,727 incident tips) in its 2025 Annual Review year, of which **204 were "nationally significant"** (up from 89) and 18 "highly significant". **Academia was the first-named sector** in the list of sectors reporting the most ransomware activity to the NCSC, ahead of finance, engineering, retail, health and manufacturing [6].

4.5 UK case evidence: disruption, data loss and recovery

Table 7. Selected UK incidents with recovery and supplier lessons

Institution / date	What happened	Impact and recovery	Lesson for resilience
British Library, Oct 2023	Rhysida ransomware; entry via a terminal server without MFA; ~600GB exfiltrated [7]	Majority of server estate encrypted or destroyed; main library platform could not be restored in pre-attack form; rebuild to mid-2024. Cloud-hosted finance, HR, payroll and email unaffected [7]	Legacy estates are the slowest to recover; cloud-hosted back-office systems contained impact. No ransom paid [7]
University of Manchester, Jun 2023	Unauthorised access; data copied, including an NHS research dataset [8]	1.1 million NHS patients from 200 hospitals in a research database; about 250GB accessed [8]	Research data shared under third-party agreements widens exposure beyond the institution
University of Cambridge (Clinical School Computing Service), Feb 2024	"Malicious activity" led to voluntary service shutdowns [9]	Medical school and CSCS websites still offline after five weeks [9]	Federated, departmental IT can lengthen recovery even when the incident is contained
Capita / USS pensions, 2023	Breach at outsourced pension administrator [16]	Members of the Universities Superannuation Scheme notified; university HR teams handled staff queries [16]	A supplier serving the whole sector creates correlated exposure
Canvas LMS (Instructure), May 2026	ShinyHunters compromise; ransom message on login pages [11][12]	UK universities including Liverpool, Queen's Belfast and Manchester were reported affected during exam season; outages from one to several days [12][54]	LMS is a tier-1 dependency at peak periods; exam contingency plans need a supplier-outage scenario
University of Nottingham, Jun 2026	Exploitation of an Oracle WebLogic vulnerability supporting the Campus Solutions (PeopleSoft) student-records system, in an isolated environment maintained by a third-party provider [10]	Contact, financial, identity and protected-characteristic data potentially accessed; system rebuilt; ICO, NCSC, OfS, UCAS and Action Fraud notified [10]	Third-party-hosted platforms still sit inside the institution's accountability; segmentation limited spread to M365 and Moodle [10]

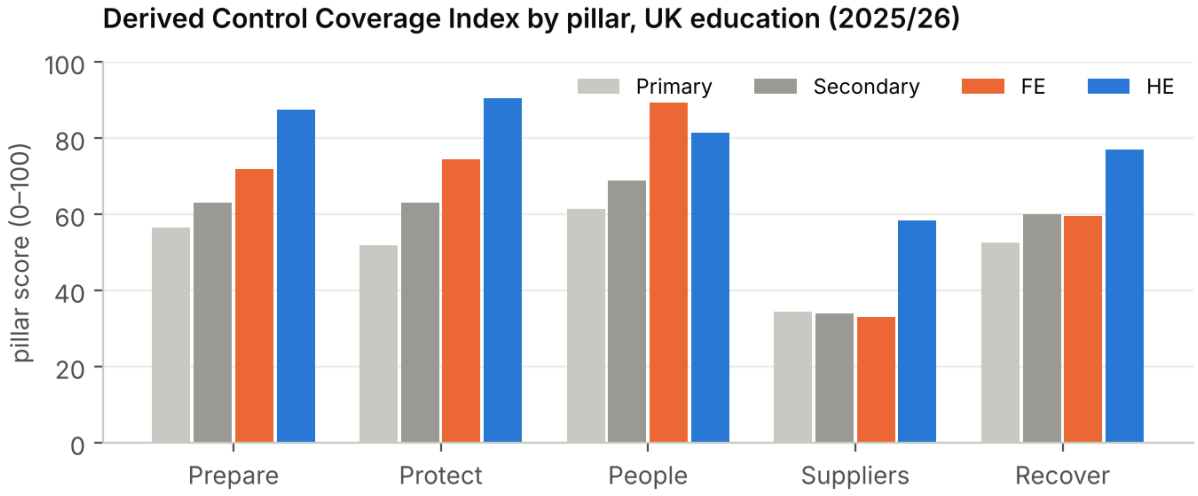
Sources as cited. Grade B (institutional disclosures) and D (media reports). Attacker claims are not treated as verified facts.

4.6 UK regulatory and policy drivers

- **Cyber Security and Resilience Bill** (introduced 12 November 2025): brings managed service providers, data centres and designated "critical suppliers" into scope, with a 24-hour initial and 72-hour full incident notification. Universities are not named as regulated entities, but their MSPs and data centres may be [52].
- **Ransomware payment ban for public bodies** (announced July 2025): covers the NHS, schools, local councils and critical services. Universities are not explicitly named; mandatory reporting is being developed [51].
- **NCSC Cyber Assessment Framework v4.0** (6 August 2025): new outcomes on understanding threats (A2.b) and assurance of software suppliers and development environments (A4.b) [53]. It is a useful benchmark for university supplier assurance even where not mandatory.
- **Office for Students reportable events:** English providers report material adverse events to the OfS, which was among the bodies Nottingham notified in 2026 [10].
- **UK GDPR:** personal-data breaches must be notified to the ICO within 72 hours where there is a risk to individuals.

5. Control coverage analysis (derived index)

Applying the index in Section 3.1 to published CSBS 2025/26 responses produces the comparative picture below. These are EQSC Global editorial calculations from secondary, published percentages [1]. They are not scores awarded to, or audited at, individual institutions.



Source: Author calculation from CSBS 2025/26 indicator percentages (unweighted means); see Section 3.1 for method.

Figure 6. Supplier governance is the weakest pillar for every type of UK education institution, including higher education.

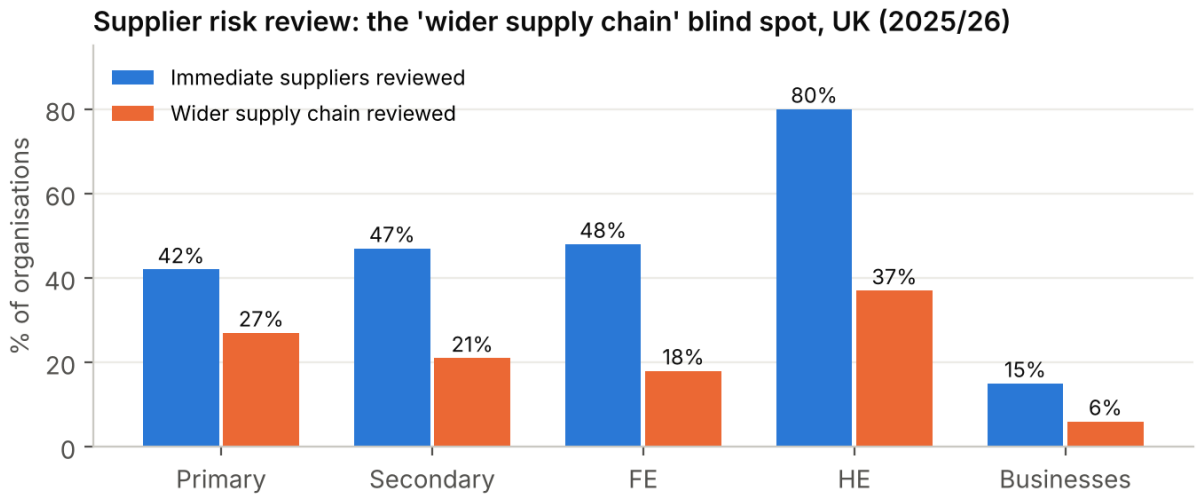
Table 8. Control Coverage Index by institution type (author calculation)

Pillar	Primary	Secondary	FE	HE
Prepare	56.5	63.2	72.0	87.5
Protect	52.0	63.0	74.5	90.5
People	61.5	69.0	89.5	81.5
Suppliers	34.5	34.0	33.0	58.5
Recover	52.7	60.0	59.7	77.0
Overall CCI (14 indicators)	50.7	57.9	66.5	81.2
Weakest single indicator	Insurance 9%	Insurance 15%	Wider supply chain 18%	Wider supply chain 37%

Figures are unweighted means of official survey percentages. The index reflects the breadth of reported control adoption, not implementation quality. The FE and HE samples have substantial margins of error (±16.2 and ±11.9 percentage points, respectively), and these uncertainties carry into any interpretation of derived scores.

Interpretation

- **HE leads overall (81.2) but has a supplier gap of 29 points below its own average.** The 43-point difference between immediate (80%) and wider (37%) supplier review is the largest internal gap in any institution type.
- **FE outperforms HE on "People" (89.5 vs 81.5)**, driven by higher awareness testing (88% vs 71%). FE, however, has much weaker protection and recovery scores and only 37% of colleges have dedicated security staff [3].
- **Recovery is the second-weakest pillar across the board.** Even in HE, only 61% hold a specific cyber insurance policy, and post-incident debriefs are not universal (84%).



Source: DSIT/Home Office, Cyber Security Breaches Survey 2025/26 – Education Institutions Findings.

Figure 7. Every type of education institution reviews the wider supply chain far less than immediate suppliers.

6. The Gulf (GCC): deep dive

6.1 Sector profile

The GCC higher education landscape includes national universities, private providers and international branch campuses whose systems may be managed in another jurisdiction. The source reports 93 Saudi higher education institutions in 2024 and approximately 1.57 million tertiary students in 2022 [46]. Dubai recorded 41 licensed providers in 2024/25, including 37 international branch campuses, with enrolment reaching 42,026 [45]. Those institutional arrangements make parent-campus contracts, data flows and recovery permissions central parts of resilience planning.

Why branch campuses matter for resilience

- A branch campus often runs identity, LMS, student records and email from the **parent institution's tenancy abroad** (for example in the UK, US, Australia or India). Its recovery time therefore depends on another country's incident response, supplier contracts and regulators.
- A parent-campus incident (for example Nottingham's 2026 Campus Solutions incident [10] or a Canvas-type LMS outage [12]) can disrupt Gulf students with no local cause and no local control over recovery.
- Data residency and reporting duties (UAE, Saudi PDPL, Qatar) may diverge from the parent's home-country rules. Incident playbooks need a **dual-jurisdiction notification matrix**.

6.2 National capability and regulation

Table 9. GCC cyber governance relevant to universities

Jurisdiction	Framework and key provisions	Relevance to universities
Saudi Arabia	NCA Essential Cybersecurity Controls ECC-2:2024 (October 2024): 4 domains, 28 subdomains, 108 controls and 92 subcontrols, including a dedicated Third-Party and Cloud Computing Cybersecurity domain (2 subdomains, 8 controls). Mandatory for government entities and CNI operators; cybersecurity roles must be filled by qualified full-time Saudi nationals [42]	Public universities are government entities and are in scope; ECC provides a ready-made control-coverage baseline
UAE	UAE Cyber Security Council with CPX published the UAE Cybersecurity Report 2025: 223,800+ exposed assets; ~50% of critical vulnerabilities unaddressed for over 5 years; misconfiguration caused 32% of incidents; 58% growth in ransomware groups operating in the UAE; DDoS fell from 58,538 (H1 2023) to 2,301 (H1 2024) [39]	Exposure and patch-latency figures are directly relevant to sprawling campus estates
UAE (2026)	Cybersecurity Council disclosed attacks targeting aviation, energy and education; Iran-linked "Static Kitten" sought access to universities via spear-phishing; Middle East organisations accounted for 8% of global academic-sector targeting (Jul 2025–Jun 2026) [41]	Confirms state-linked interest in Gulf academic research and IP
GCC-wide	ITU Global Cybersecurity Index 2024: Saudi Arabia, UAE, Qatar, Oman and Bahrain among 46 Tier 1 "role-modelling" countries [43]	Strong national capacity does not by itself measure institution-level readiness

Grades A–B. Where provisions are summarised from secondary legal commentary, readers should confirm against the regulator's published text.

6.3 Threat tempo

Positive Technologies reported that the UAE accounted for 35% of cyberattacks in a wider Gulf-region dataset for the first half of 2026, with Iran at 17% and Saudi Arabia at 15% [40]. Because Iran is not a GCC member, these shares must not be presented as a GCC-only distribution. The vendor attributed a marked concentration of incidents in the first quarter to wider regional developments. Government organisations were the largest named affected group; education was not separately quantified, so the findings cannot establish the university-specific attack rate.

Table 10. Ransomware and breach economics, UAE and Middle East

Indicator	Value	Source
UAE ransomware victims fully recovered within one week (2025)	63%	[24]
UAE victims whose data was encrypted	55%	[24]
UAE: data also stolen where encrypted	43% (global 28%)	[24]
UAE victims paying ransom	43%; median payment US$1.33m	[24]
UAE mean recovery cost excl. ransom	US$1.41m	[24]
UAE root cause: exploited vulnerabilities	42%	[24]
Middle East average breach cost (IBM 2025)	SAR 27.0m (down 18% from SAR 32.8m)	[38]
Middle East orgs with AI access controls	41% (global 3%, as reported)	[38]

Sophos UAE data are cross-sector (organisations with 100–5,000 employees). IBM figures cover the Saudi/UAE cluster. Grade C.

6.4 Evidence gap: the central Gulf finding

The central finding for the GCC is an evidence gap. National frameworks and public discussion of cyber incidents offer useful context, yet no recurring, comparable institution-level university resilience dataset was identified in the sources reviewed. Publicly observable recovery times, training outcomes and supplier-concentration measures are correspondingly limited. This is a strong case for carefully authorised primary measurement, especially among international branch campuses.

- Use **ECC-2:2024** (Saudi) and the relevant national information assurance standards (UAE, Qatar) as the control list for non-intrusive coverage reviews, mapped to the CCI pillars.
- Survey branch campuses separately from national universities, and record which tier-0 services are run from the parent campus abroad.
- Measure dependence on regional cloud regions and national sovereign-cloud requirements as part of supplier concentration.

7. India: deep dive

7.1 Sector profile

India's higher education system operates at exceptional institutional scale. AISHE 2021–22 recorded 1,168 universities, 45,473 colleges, 12,002 standalone institutions and 43.3 million students [47]. The Ministry of Education released AISHE 2022–23 and 2023–24 on 8 July 2026; the latter reported 45.0 million enrolments [48]. Affiliated colleges often depend on central university examination, results and admissions portals, so disruption to one shared service may reach many campuses.

7.2 Threat intensity

Table 11. India: threat and breach indicators

Indicator	Value	Source
Weekly attacks per education organisation, India (2025)	8,487	[29]
Weekly attacks per education organisation, global (2025)	4,368	[29]
India education vs global education (author calc.)	1.94x	derived
India education vs other Indian industries (3,278/week) (author calc.)	2.59x	derived
Weekly attacks per organisation, India, all sectors (Aug 2025)	3,237 (global 1,994)	[30]
Cyberattacks on Indian educational institutions, Jul 2023–Apr 2024	200,000+	[31]
Data breaches affecting Indian educational institutions, same period	nearly 400,000	[31]
Unique usernames / passwords seen in brute-force attempts	8,000+ / 54,000+	[31]
Incidents handled by CERT-In (2025, all sectors)	29.44 lakh (2.94 million)	[32]
India average breach cost (IBM 2025)	INR 220m (+13%); 263-day lifecycle	[37]
India top breach vectors (IBM 2025)	Phishing 18%; third-party/supply chain 17%; vulnerability exploitation 13%	[37]
Indian ransomware victims paying (Sophos 2025)	53%; median US$481,636	[25]
Indian mean recovery cost excl. ransom	US$1.01m	[25]

Check Point and CyberPeace observations are telemetry or research-network measures (Grade D); they are not directly comparable to statutory CERT-In incident counts or IBM survey estimates. The CyberPeace use of "data breaches" concerns observed leak records, which should not be mistaken for confirmed, separately investigated institutional incidents.

In IBM's 2025 India study, **third-party vendor and supply-chain compromise (17%)** was almost as common an initial vector as phishing (18%) [37]. The CyberPeace e-Kawach study, run with DELNET and other partners, reported consequences specific to education: faculty impersonation, deepfake content, theft of research data and **exam-paper leakage** [31].

7.3 Regulatory clocks and obligations

Table 12. Indian obligations relevant to university incident response

Instrument	Key requirement	Implication for universities
CERT-In Directions (28 April 2022)	Report specified incidents (20 types) within 6 hours of noticing; retain ICT logs for 180 days in India; synchronise clocks to NIC/NPL NTP; designate a Point of Contact. Non-compliance: up to 1 year imprisonment or INR 1 lakh fine [33]	Requires 24x7 triage and decision capability, which is hard for colleges without security staff
DPDP Act 2023 & Rules 2025 (notified 13 Nov 2025)	Breach notice to affected individuals without delay and a detailed report to the Data Protection Board within 72 hours; reasonable security safeguards incl. MFA for privileged users and one-year log retention; verifiable parental consent for under-18s; penalties up to INR 250 crore. Substantive obligations enforceable from 13 May 2027 [34]	Universities process data on minors (first-year students, school outreach) and must budget for consent and safeguards
CERT-In Comprehensive Cyber Security Audit Policy Guidelines (25 July 2025)	Comprehensive ICT audit at least annually by CERT-In-empanelled auditors; scope includes vendor risk management, cloud, AI and SBOM; reports to CERT-In within 5 days [35]	Provides an external control-coverage measurement route; 231 empanelled audit organisations available [32]
UGC Handbook on Basics of Cyber Hygiene for HEIs (2025)	Promotes cyber awareness, digital safety and data-privacy education across courses, following a Parliamentary Standing Committee recommendation [36]	Supports training uptake; does not by itself mandate technical controls

Some provisions are summarised from secondary legal commentary. The original CERT-In directions and MeitY notifications are the appropriate sources for operational decisions; applicability, commencement and notification obligations require confirmation by institutional counsel. This report is not legal advice.

National exercising capacity is substantial: CERT-In conducted **122 cybersecurity drills and exercises** with about **1,570 organisations** in 2025 [32]. Universities are not separately reported, and higher education has no sectoral CSIRT comparable to CSIRT-Fin or CSIRT-Power [32]. Creating one, or a Jisc-style shared service for HEIs, is one of this report's recommendations.

7.4 The Indian resilience gap in one sentence

Summary

Indian universities face roughly twice the global education attack rate and the world's shortest statutory reporting clock, yet the sector has no official measure of institutional cyber posture, no sector CSIRT and a highly federated estate. Measurement (Annex A–C) and shared response capacity are the two highest-leverage interventions.

8. Technology dependencies and supplier concentration

Many university services now depend on hosted software, cloud infrastructure or external administrators. That model can improve security and restoration, as the British Library incident review illustrates for some unaffected cloud-hosted back-office systems [7]. It can also introduce common-mode failures: several universities may lose the same service at once, while each has limited ability to determine how rapidly the supplier restores it.

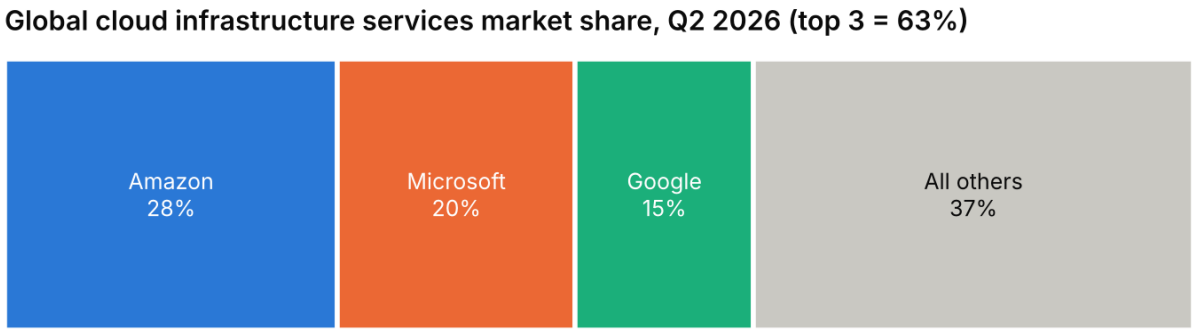
8.1 Sector-wide supplier incidents

Table 13. Supplier and platform incidents with sector-wide impact

Supplier / year	Mechanism	Scale in education	Resilience lesson
Instructure Canvas LMS, Apr–May 2026	Unauthorised access from 25 April; detected 29 April; second attack 7 May displayed a ransom message on login pages; agreement with attackers reached 11 May [12]	8,809 institutions worldwide; Canvas used by ~41% of North American HE [11][11][12][55][56]; attackers claimed 275 million users (unverified) [11][12][55][56]	Peak-period LMS dependency; need for offline exam fallbacks and contractual breach-notification clocks
Oracle E-Business Suite zero-day (CVE-2025-61882), Aug–Nov 2025	Clop exploited a zero-day in on-premises EBS from early August; patch issued 4 October 2025 [14]	University of Pennsylvania and Dartmouth College among confirmed victims; finance, procurement and supplier-payment data [14]	ERP platforms are high-value targets; patch latency on enterprise apps is a recovery-time driver
National Student Clearinghouse (MOVEit), 2023	Exploitation of MOVEit Transfer at a shared data intermediary [13]	~890 US colleges and universities had data stolen [13]	Fourth-party risk: institutions were breached through a supplier's supplier
Blackbaud, 2020	Ransomware and data theft at a hosted CRM/fundraising provider [15]	Multiple UK and North American universities affected; full client list not disclosed [15]	Advancement/alumni data held by suppliers is still the institution's data
Capita (USS pensions), 2023	Breach at outsourced administrator [16]	Universities Superannuation Scheme members across UK HE [16]	Sector-wide shared suppliers concentrate risk
PowerSchool, Dec 2024	Compromised credential used on a customer support portal [17]	16,000 UK students across four schools; reportedly 62m students globally (unconfirmed) [17]	Supplier support channels are an attack path; supplier declined to file with the ICO, claiming it was not a data controller [17]
CrowdStrike Falcon update, 19 July 2024	Faulty content update crashed Windows hosts (no attack) [18]	8.5 million Windows devices globally, including university estates [18]	Non-malicious supplier failure is also a resilience event; recovery needed hands-on device remediation

Sources as cited. Grade B/D. Attacker claims are reported as claims.

8.2 Measuring concentration



Source: Synergy Research Group, Q2 2026 cloud market release. Partial HHI from top three alone = 1,409 (author calculation).

Figure 8. Three providers hold 63% of global cloud infrastructure; most university tier-0 services depend on one of them.

Synergy Research Group reported Q2 2026 cloud infrastructure shares of 28% for Amazon, 20% for Microsoft and 15% for Google, within a US$143.4 billion quarterly market [19]. Their combined share is 63%; the partial HHI contribution of those three alone is 1,409 ($28^2 + 20^2 + 15^2$, EQSC Global calculation). These market shares describe global cloud infrastructure, not university-specific hosting. Estimates of 41% Canvas use among North American HE and around 70% SITS:Vision use among UK HE are cited from secondary sources and should be verified before being used for procurement decisions [11][20].

8.3 Worked example: institution-level HHI

Market concentration alone does not reveal the exposure of a particular university. A more useful operational question is how many of its foundational and mission-critical services depend on the same provider. The hypothetical example below maps ten services to five supplier slots; it demonstrates the calculation and describes no actual institution.

Table 14. Illustrative calculation (hypothetical service map, not real data)

Supplier (hypothetical)	Tier-0/1 services provided (of 10)	Share squared
Cloud/productivity provider A (identity, email, storage, Teams/collab)	4 (40%)	1,600
LMS provider B	1 (10%)	100
Student-records provider C (hosted)	2 (20%)	400
ERP provider D (finance, HR/payroll)	2 (20%)	400
Network/security MSP E	1 (10%)	100
Institution HHI		2,600 (highly concentrated)

Method: HHI = Σ(share%)². Above 2,500 = high concentration. Annex A, Q-SC3 collects the inputs.

Supplier concentration is not inherently undesirable. A well-managed common platform may improve availability and reduce duplication. The issue is whether the institution also has realistic recovery rights: prompt incident notification, access to useful logs, tested exports, workable exit arrangements and manual contingencies for critical academic periods.

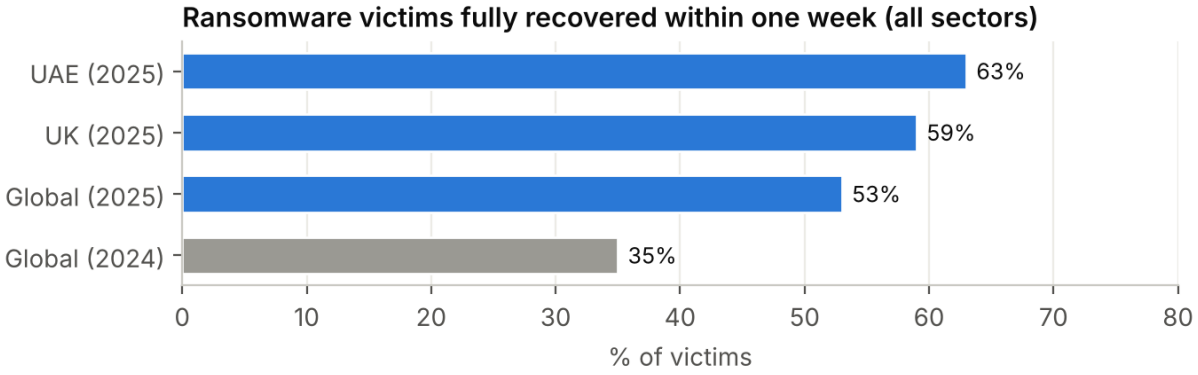
8.4 Service exposure: where dependency meets the calendar

Table 15. Service exposure scoring template (with indicative ratings)

Service	Criticality (1–5)	Attack surface (1–5)	Supplier dependency (1–5)	Peak sensitivity (1–3)	Exposure (max 375)
Identity / SSO	5	5	4	3	300
LMS / VLE	5	5	5	3	375
Student records (SIS)	5	3	4	3	180
Admissions / CRM	4	4	4	3	192
Finance / ERP	4	3	4	1	48
Research data storage	4	3	3	1	36

Scores are deliberately indicative and illustrate the multiplication method rather than an assessment of any real campus. Each institution should set its own ratings using a documented business impact assessment; peak sensitivity is higher during periods such as enrolment, examinations and results.

9. Recovery capability



Source: Sophos State of Ransomware 2025 – global, UK and UAE editions. Cross-sector; no India figure published in the sources reviewed.

Figure 9. Faster recovery is now the norm across sectors: more than half of ransomware victims recover fully within a week.

In the Sophos cross-sector ransomware studies, the share of respondents reporting full recovery within one week increased from 35% in 2024 to 53% in 2025, while recoveries taking longer than a month fell from 34% to 18% [23]. The comparable cited figures were 59% in the UK and 63% in the UAE [23][24]. The source review did not identify a published, comparable India-specific recovery-time statistic or country-level university recovery distributions. Annex B describes how those gaps could be addressed through authorised incident records.

9.1 What determines recovery time

Table 16. Recovery drivers and the evidence behind them

Driver	Evidence	Implied control
Backup integrity	Backups targeted in 95% of education attacks; 71% of attempts succeeded [22]. HE backup-based restoration fell to 47% [21]	Immutable/offline copies; separate backup identity; restore testing
Legacy and on-premises estate	British Library: legacy infrastructure and terminal server without MFA; core platform not restorable in pre-attack form [7]	Legacy retirement roadmap; cloud migration of back-office
Segmentation	Nottingham: compromised SIS environment was isolated; M365 and Moodle unaffected [10]	Network and tenant segmentation of tier-1 systems
Federated IT	Cambridge CSCS: departmental services offline for five weeks [9]	Central minimum standards for departmental IT
Detection speed	IBM: India breach lifecycle 263 days [37]	Monitoring, threat hunting, log retention (180 days CERT-In; 1 year DPDP)
Expertise and capacity	Sophos: 66% of education victims cited insufficient personnel [21]; 37% of UK FE colleges have dedicated security staff [3]	Retainer with an incident response provider; sector shared services

Sources as cited.

9.2 Lessons from the British Library review

The British Library's public incident review is unusually detailed and offers lessons relevant to universities, although the British Library is not itself a university. Its account of disrupted services,

legacy infrastructure and restoration planning can be mapped to the five resilience measures used here [7].

British Library lesson (abridged)	Metric
Enhance network monitoring; retain external security expertise; strengthen intrusion response	Control coverage; response resources
Implement universal MFA; network segmentation	Control coverage
Practise comprehensive business continuity; balance security with recovery investment	Recovery time
Maintain a holistic cyber-risk overview; eliminate and prioritise legacy technology	Service exposure
Build cyber expertise at senior levels; regular staff training; support staff and user wellbeing; review acceptable-use policies	Training uptake; response resources
Collaborate with sector peers; implement and audit government standards regularly	Control coverage; supplier concentration

10. Staff awareness and response resources

10.1 Training uptake vs training effectiveness

Table 17. Training and testing indicators

Indicator	Value	Source
UK HE delivering cyber training (2025/26)	92% (FE 91%, secondary 77%, primary 72%)	[1]
UK HE running staff-awareness testing	71% (2025: 94%)	[1][2]
UK FE running staff-awareness testing	88%	[1]
Phishing among UK FE/HE breaches	96%	[1]
Impersonation among UK FE/HE breaches	79%	[1]
Global baseline phish-prone percentage (untrained)	33.1%	[27]
After 90 days of training	~20% reduction	[27]
After 12 months of training	86% reduction (~4.1%)	[27]
Compromised UK education credentials (12 months to Jun 2026)	144,000+ (three-fold rise)	[4]
Stolen credentials as leading breach vector (global)	22% of breaches	[26]

KnowBe4 benchmark: 67.7 million simulations, 14.5 million users, 62,400 organisations; no education-specific value published in the source [27].

The UK evidence suggests that training coverage alone is an incomplete measure of staff readiness. HE institutions report high participation in training, yet the share undertaking awareness tests fell substantially between survey waves [1][2]. Whether this reflects sampling or a genuine change, institutions need direct evidence of user behaviour. A useful dashboard should include completion, click and reporting rates, plus role-specific exercises for privileged users.

1. **Uptake:** % of staff (and postgraduate researchers with system access) completing training in 12 months.
2. **Click rate:** % of simulated phishing emails clicked, measured quarterly.
3. **Report rate:** % of simulated phishing emails reported to the security team. This is the best leading indicator of a "human sensor" network.
4. **Privileged-user readiness:** % of administrators completing role-specific training and an incident drill in 12 months.

10.2 Response resources

Table 18. Response resources by region (best available indicators)

Resource	UK	Gulf / India
Dedicated security staff	HE 92%; FE 37% [3]	Not published for universities; ECC-2:2024 requires qualified full-time Saudi nationals in cyber roles [42]
Sector CSIRT / shared service	Jisc CSIRT and Janet network; 16,000+ incidents recorded in 2025 [3]	India: CERT-In plus sectoral CSIRTs (finance, power) but no HE CSIRT [32]; Gulf: national CERTs

Resource	UK	Gulf / India
National exercising	NCSC Exercise in a Box (free tabletop tool)	India: 122 CERT-In drills with ~1,570 organisations in 2025 [32]
Cyber insurance	HE specific policy 61%; any cover 69% [1]	No published HE data
Board oversight	HE: 100% have a board member responsible; 84% update governors quarterly+ [1]	No published HE data
External audit	Pen testing in 84% of HE [1]	India: annual CERT-In-empanelled audit expected; 231 empanelled auditors [32][35]

NCSC Exercise in a Box is a free NCSC tool for tabletop exercises; no usage statistic for HE is cited.

11. Cross-regional comparison

This cross-regional scorecard is an interpretation of the evidence in Sections 4–10, not a league table derived from matched institutional observations. The categories “Stronger”, “Mixed” and “Weaker” describe relative signals within the available sources; “Unknown” means the evidence does not support a defensible comparison. Differences in survey definitions and the limited HE-specific data outside the UK prevent precise international rankings.

Table 19. Regional resilience scorecard (analyst judgement)

Metric	United Kingdom	Gulf (GCC)	India
Recovery time	Mixed. 59% of ransomware victims recover within a week [23]; HE backup restoration weak globally [21]	Stronger (cross-sector). 63% within a week in UAE [24]; no HE data	Unknown. No published recovery-time data; 263-day breach lifecycle [37]
Control coverage	Stronger. HE CCI 81.2; 98% MFA; 92% IR plans [1]	Mixed. Strong mandated frameworks (ECC-2:2024) [42]; 50% of critical vulns >5 years old (UAE) [39]	Weaker/unknown. Annual audit guidance new (2025) [35]; brute-force exposure widespread [31]
Supplier concentration	Weaker. Wider supply-chain review 37% (HE) [1]; LMS/SIS concentration [12][20]	Mixed. ECC third-party & cloud domain [42]; branch-campus dependency on parents abroad [45]	Weaker. Third-party compromise 17% of breaches [37]; university-portal hub-and-spoke model
Training uptake	Stronger on reach (92% HE) [1]; effectiveness measurement slipping	Unknown	Mixed. UGC cyber-hygiene handbook [36]; no uptake data
Service exposure	Mixed. 49% of FE/HE breaches caused negative outcomes [1]; 144k leaked credentials [4]	Weaker. 223,800 exposed UAE assets [39]; 35% of Gulf attacks on UAE [40]	Weaker. 8,487 weekly attacks per education organisation [29]
Evidence availability	High (official statistics, Jisc, NCSC)	Low (national data; little HE-specific)	Low–medium (telemetry, CERT-In aggregates)

Qualitative assessments are EQSC Global editorial judgements based on available secondary evidence. They should be replaced by standardised, measured results if primary institutional data become available.

11.1 Regulatory clocks compared

Table 20. Incident notification timelines

Regime	Clock	Scope
India -CERT-In Directions 2022	6 hours	Specified cyber incidents, all covered entities [33]
UK -Cyber Security and Resilience Bill (proposed)	24h initial / 72h full	Regulated entities incl. MSPs, data centres (not universities by default) [52]
India -DPDP Rules 2025	Without delay to individuals; 72h to Board	Personal-data breaches; enforceable from 13 May 2027 [34]
UK -UK GDPR	72 hours	Personal-data breaches posing risk to individuals (ICO)

Regime	Clock	Scope
India -CERT-In audit report submission	5 days	After annual audit [35]

Gulf notification timelines vary by jurisdiction and regulator and were not verified for this edition; institutions should confirm with the relevant national authority.

12. Modelled benchmark study (illustrative)

How to read this section

- **Everything in Section 12 is modelled, synthetic data.** It shows what the primary study in Annexes A–C would produce. It is not a record of real institutions, incidents or exercises, and it must not be cited as observed fact.
- **The data are calibrated to real benchmarks.** Control-adoption probabilities for UK universities and colleges use the CSBS 2025/26 percentages [1]. Ransomware recovery times are tuned to the Sophos 2025 within-one-week figures [23][24], and the supplier-origin share of incidents to the Verizon DBIR third-party share [26]. Gulf and India parameters are analyst assumptions informed by Sections 6–7.
- The source report describes a fixed simulation seed (20261007) and refers to a companion workbook containing 240 institutions, 544 incidents and 60 exercises. That workbook was not included among the materials supplied for this publication edit; its figures are reproduced here from the report but could not be recomputed independently.
- Every modelled chart carries a red "MODELLED DATA -ILLUSTRATIVE" stamp, and every modelled table title begins with "Modelled".

12.1 Model design

Table 24. Modelled sample frame

Region	Segment	n	Calibration basis
UK	University (HE)	50	CSBS 2025/26 HE percentages [1]
UK	FE college	30	CSBS 2025/26 FE percentages [1]; Jisc staffing [3]
Gulf	National university	40	Assumed: strong frameworks (ECC-2:2024) [42], moderate implementation
Gulf	International branch campus	30	Assumed: parent-campus controls, high supplier concentration [45]
India	Public university	40	Assumed: constrained resources; India threat data [29][31]
India	Private university	25	Assumed: mid-range investment
India	Affiliated college	25	Assumed: minimal dedicated security capacity

Total n = 240 institutions. Incidents were simulated as Poisson counts over a 24-month window. Recovery hours were drawn from log-normal distributions whose medians shift with incident type, region and the institution's controls.

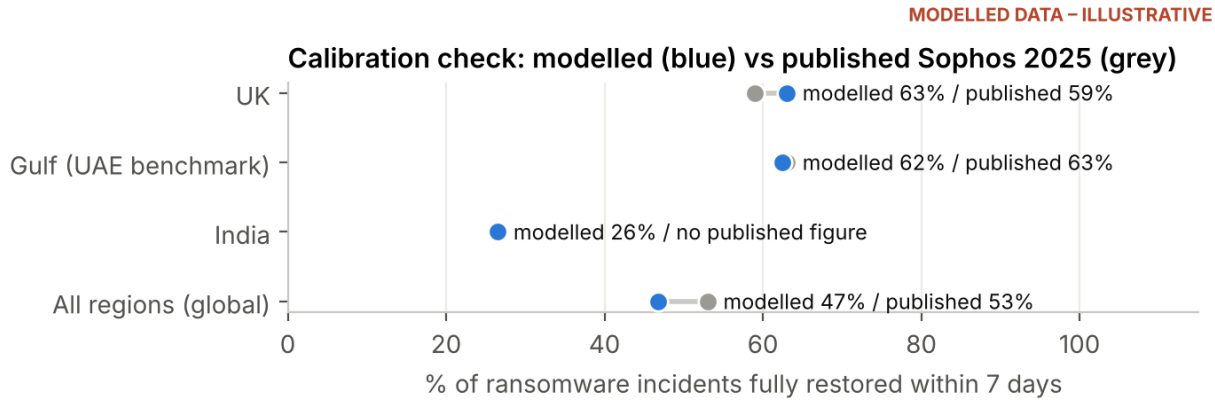
Table 25. Modelled variables and links to the five metrics

Variable	How it was modelled	Metric
16 binary controls	Bernoulli draws with segment-specific probabilities (UK anchored to CSBS 2025/26)	Control coverage

Variable	How it was modelled	Metric
Hours to minimum service / full restoration	Log-normal; type medians from 7h (DDoS) to ~70h (ransomware); multipliers for backups, tested IR plan, segmentation, supplier clauses, region and peak period	Recovery time
Supplier HHI	Dirichlet allocation of 10 tier-0/1 services across 5 supplier slots	Supplier concentration
Training uptake, click and report rates	Truncated normal by segment; report rate falls as click rate rises	Training uptake
Maximum service exposure score	Truncated normal, 0–375 scale (Table 15)	Service exposure
Tabletop scores	10 criteria scored 0–3; mean rises with CCI; penalties where no notification clause or restore test	All five

12.2 Calibration check

MODELLED DATA -ILLUSTRATIVE. The synthetic dataset was calibrated against public benchmarks as a reasonableness check, not validated against observed institutional records. In the model, 63% of UK ransomware incidents were fully restored within seven days, compared with 59% in the cited UK cross-sector study [23]. The Gulf synthetic result was 63% against 63% in the UAE benchmark [24], while the all-region result was 47% against a global figure of 53% [23]. Supplier/platform failures represented 31.8% of simulated incidents, close to the 30% third-party breach share reported in the Verizon analysis [26]. These similarities reflect calibration choices, not independent predictive accuracy.



Source: Modelled dataset vs Sophos State of Ransomware 2025 (UK, UAE, global; cross-sector). Grey = published benchmark.

Figure 10 (modelled). Modelled ransomware recovery rates sit within a few points of the published Sophos 2025 benchmarks.

12.3 Modelled headline results by region

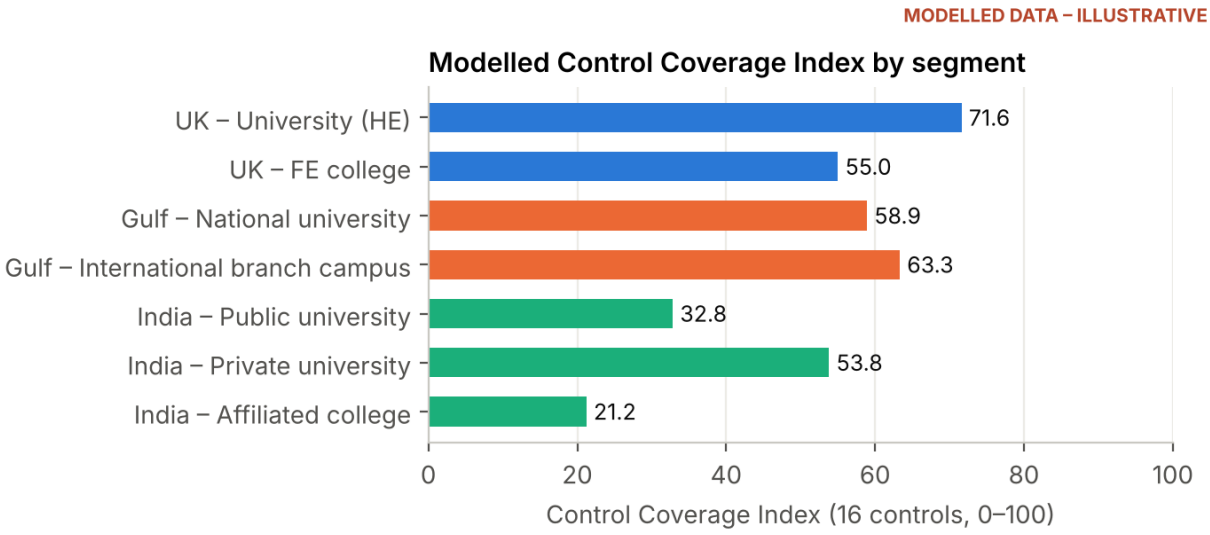
Table 26. Modelled regional scorecard (all five metrics)

Measure (modelled)	UK	Gulf	India
Institutions in model	80	70	90
Control Coverage Index (16 controls)	65.4	60.8	35.4
Disruptive incidents per institution (24 months)	2.3	2.0	2.4
Median hours, detection to declaration	3.1	2.8	7.5

Measure (modelled)	UK	Gulf	India
Median hours to minimum service	15.8	18.7	25.3
90th percentile hours to minimum service	65.0	66.7	123.6
Median hours to full restoration	43.3	55.8	88.7
Incidents meeting tier-1 RTO (UK/Gulf 48h; India 72h)	79.6%	81.1%	78.6%
Supplier/platform-originated incidents	34.9%	31.5%	29.3%
Median supplier HHI (tier-0/1)	3,400	4,200	3,400
Training uptake (mean)	87.3%	75.6%	53.3%
Phishing click rate / report rate	9.3% / 41.5%	13.2% / 35.1%	21.6% / 25.4%
Mean maximum service exposure (0–375)	236	244	234
Mean tabletop score (0–30)	21.0	20.5	16.7

MODELLED DATA -ILLUSTRATIVE. India's looser 72h RTO explains why its RTO attainment is similar to the UK's despite slower recovery.

12.4 Control coverage (modelled)



Source: Modelled benchmark dataset (synthetic, n=240 institutions; 24-month incident window), calibrated to published benchmarks. Not observed data.

Figure 11 (modelled). Coverage varies more within regions than between them; Indian affiliated colleges and public universities sit far below their private peers.

MODELLED DATA -ILLUSTRATIVE. The modelled UK university CCI (71.6) is lower than the CSBS-derived 81.2 in Section 5 because the modelled control set is stricter. It adds privileged access management, 24x7 monitoring, immutable backups, restore testing and supplier contract clauses, which official surveys do not measure. The largest within-region gap is in India: private universities (53.8) against affiliated colleges (21.2).

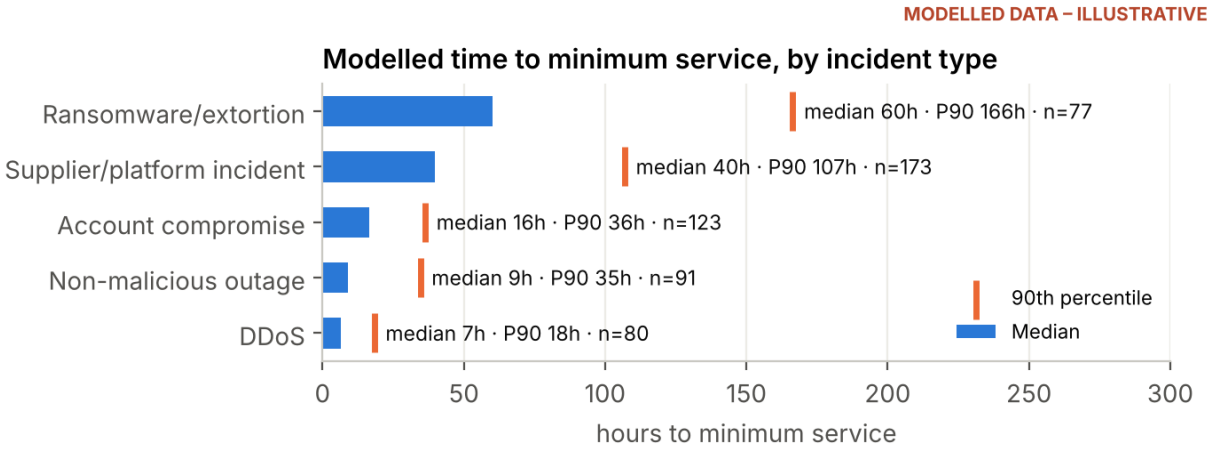
Table 27. Modelled control adoption by region (% of institutions)

Control	UK	Gulf	India
MFA for all staff	99%	96%	62%
Critical patches within 14 days	81%	77%	39%

Control	UK	Gulf	India
Endpoint detection & response	90%	80%	58%
24x7 security monitoring	60%	69%	37%
Tier-1 network segmentation	57%	61%	38%
Privileged access management	55%	61%	31%
IR plan tested (12 months)	66%	59%	30%
BCP covers cyber	85%	79%	50%
Immutable/offline backups	49%	60%	19%
Full restore test (12 months)	57%	43%	30%
Immediate supplier review	71%	64%	37%
Wider supply-chain review	28%	24%	13%
24h supplier notification clause	30%	29%	14%
Training delivered	90%	81%	57%
Phishing simulation	70%	51%	41%
Specific cyber insurance	57%	39%	11%

MODELLED DATA -ILLUSTRATIVE.

12.5 Recovery time (modelled)



Source: Modelled benchmark dataset (synthetic, n=240 institutions; 24-month incident window), calibrated to published benchmarks. Not observed data.

Figure 12 (modelled). Ransomware and supplier incidents dominate recovery time; supplier incidents are the most frequent long-duration event.

Table 28. Modelled recovery by incident type

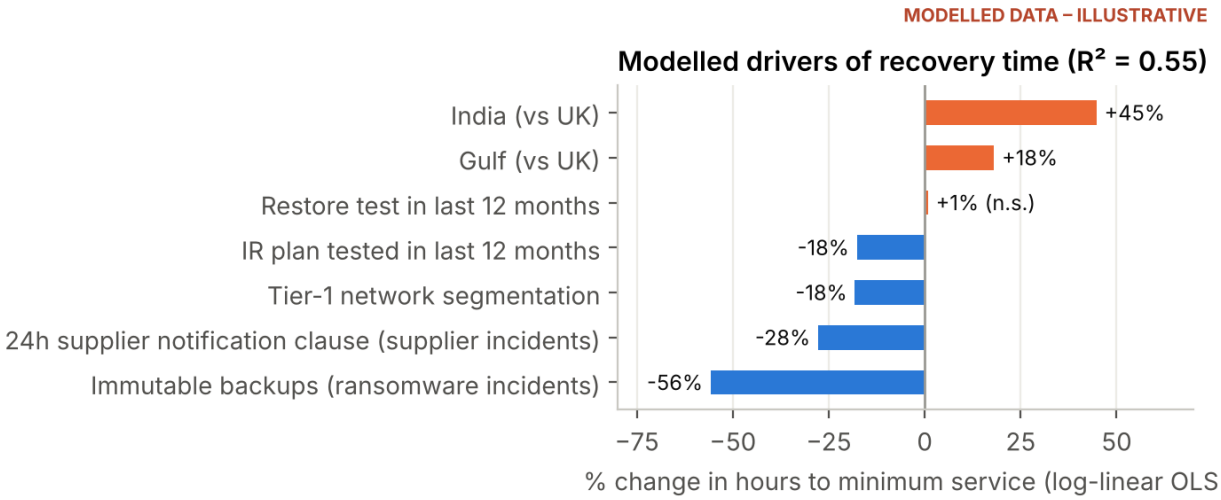
Incident type	n	Median h to min. service	P90 h	Median h to full restore	Met RTO
Ransomware/extortion	77	60.3	166.4	184.3	45.5%
Supplier/platform incident	173	39.8	106.9	126.5	62.4%
Account compromise	123	16.4	36.3	43.3	98.4%

Incident type	n	Median h to min. service	P90 h	Median h to full restore	Met RTO
Non-malicious outage	91	8.9	34.6	27.7	97.8%
DDoS	80	6.6	18.3	21.7	100.0%

MODELLED DATA -ILLUSTRATIVE.

MODELLED DATA -ILLUSTRATIVE. Supplier and platform incidents were the most common disruptive event in the model (173 of 544). Only 62.4% of them met the tier-1 RTO, compared with 45.5% for ransomware and more than 97% for DDoS, account compromise and non-malicious outages.

What shortens recovery? (modelled driver analysis)



Source: Modelled dataset; OLS on log(hours to minimum service) with incident-type controls. n.s. = |t|<1.96. Effects reflect modelling assumptions.

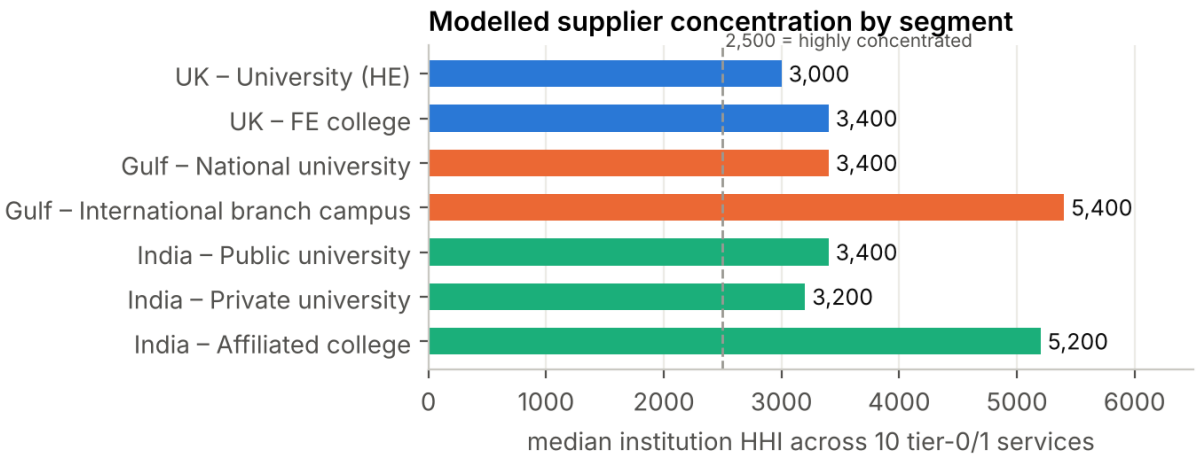
Figure 13 (modelled). Immutable backups, supplier notification clauses, segmentation and tested IR plans are associated with materially shorter recovery.

- **MODELLED DATA -ILLUSTRATIVE. Immutable backups:** for ransomware incidents, -56% hours to minimum service. The median was 31.8h with immutable backups (n=28) against 87.0h without (n=49).
- **24-hour supplier notification clause:** for supplier incidents, -28%. The median was 32.1h with the clause against 48.2h without.
- **Tier-1 segmentation:** -18%. **Tested IR plan:** -18% (median 16.8h vs 26.2h across all incidents).
- **Supplier concentration:** supplier incidents at institutions in the top HHI third (≥4,200) took a median 51.9h to minimum service, against 34.9h in the bottom third (≤3,000).
- **Restore testing** showed no independent effect (+1%, not significant) once immutable backups were controlled for. In a real study this would merit investigation: testing may matter mainly through the backup quality it reveals.
- **Region:** India +45% and Gulf +18% versus the UK, after controls (model R^2 = 55.4%).

MODELLED DATA -ILLUSTRATIVE. The reported associations partly arise from parameters deliberately built into the simulation. They are examples of analyses that could be undertaken with consented real-world data; they do not establish causal effects or measured recovery benefits for universities.

12.6 Supplier concentration (modelled)

MODELLED DATA – ILLUSTRATIVE



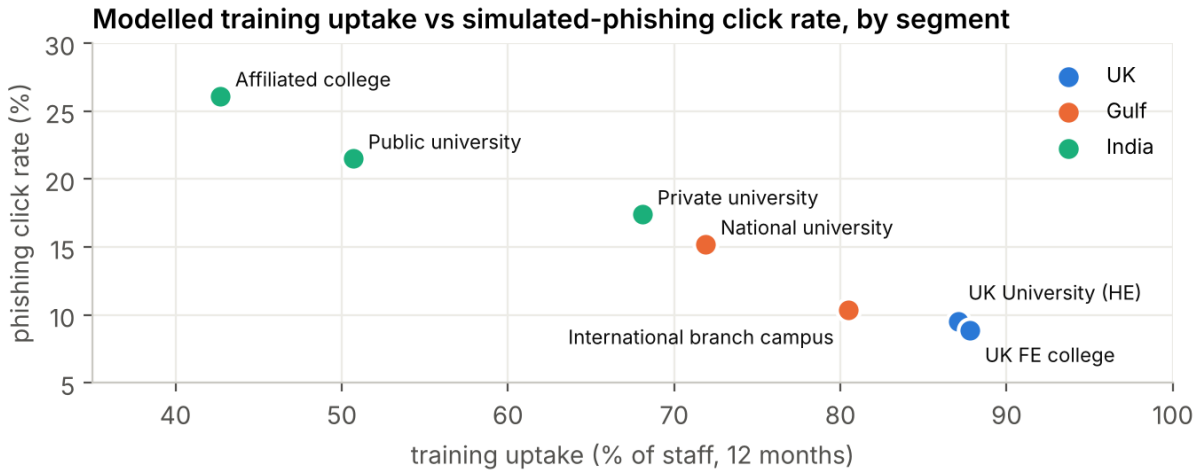
Source: Modelled benchmark dataset (synthetic, n=240 institutions; 24-month incident window), calibrated to published benchmarks. Not observed data.

Figure 14 (modelled). Every segment is above the 2,500 high-concentration line; branch campuses and affiliated colleges are the most concentrated.

MODELLED DATA -ILLUSTRATIVE. International branch campuses (median HHI 5,400) and Indian affiliated colleges (5,200) were the most concentrated segments. Branch campuses draw most tier-0/1 services from the parent institution's tenancy, and colleges depend on the affiliating university's portals. Wider supply-chain review was rare in both segments (17% and 4%).

12.7 Training uptake and effectiveness (modelled)

MODELLED DATA – ILLUSTRATIVE



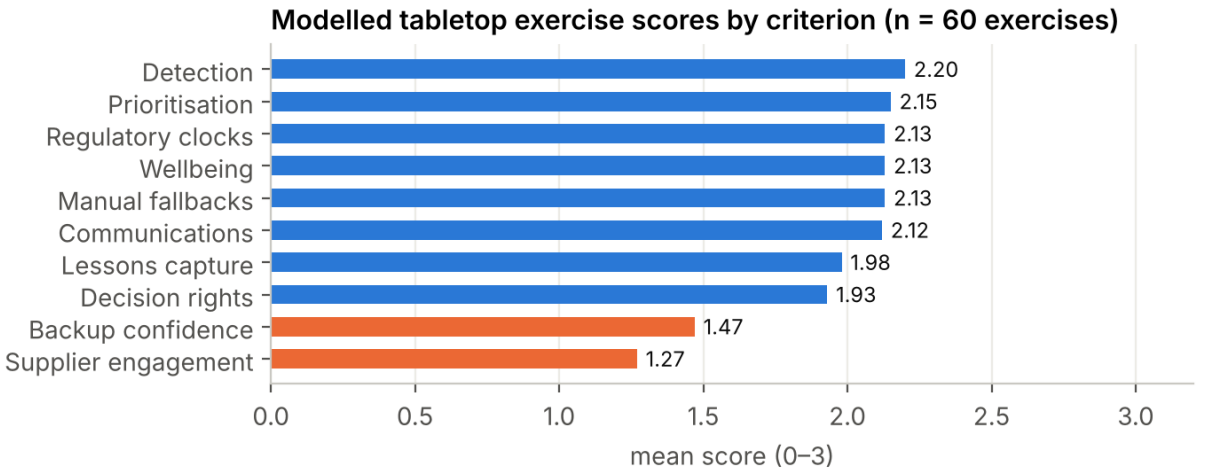
Source: Modelled benchmark dataset (synthetic, n=240 institutions; 24-month incident window), calibrated to published benchmarks. Not observed data.

Figure 15 (modelled). Higher training uptake is associated with lower simulated-phishing click rates across segments.

MODELLED DATA -ILLUSTRATIVE. Mean training uptake ranged from 42.7% (Indian affiliated colleges) to 87.8% (UK FE colleges), and click rates ran from 8.9% to 26.1%. Report rates were below 45% in every segment. This suggests the "human sensor" metric recommended in Section 10.1 has the most room to improve.

12.8 Tabletop exercise results (modelled)

MODELLED DATA – ILLUSTRATIVE



Source: Modelled benchmark dataset (synthetic, n=240 institutions; 24-month incident window), calibrated to published benchmarks. Not observed data.

Figure 16 (modelled). Supplier engagement and backup confidence are the weakest-scoring tabletop criteria.

MODELLED DATA -ILLUSTRATIVE. Of 60 modelled exercises, 7 scored "resilient" (25–30), 35 "developing" (18–24) and 18 "at risk" (below 18). Exercise totals were strongly correlated with CCI (r = 0.78). The two weakest criteria were **supplier engagement** (mean 1.27 of 3) and **backup confidence** (1.47). This matches the published evidence that supplier governance and backup integrity are the sector's soft spots [1][22].

12.9 What a primary study could test

Modelled insights to test with real data

- Supplier incidents are likely to be the **most frequent cause of long outages**, not ransomware. Modelled: 173 supplier incidents against 77 ransomware incidents.
- A **24-hour supplier notification clause** may be among the cheapest recovery-time interventions available.
- Immutable backups appear to be the **single largest lever** on ransomware recovery.
- India's gap is driven by **segment mix** (affiliated colleges, public universities) as much as by region. Targeted support for colleges would move national averages most.
- Branch campuses look strong on controls but weak on **supplier independence**. Their resilience is largely set by the parent institution.

13. Recommendations and roadmap

13.1 For university leadership and governing bodies

1. **Own the recovery objective, not just the risk.** Approve RTO/RPO targets for tier-0 and tier-1 services (Section 3.2) and require an annual report of tested versus target recovery times.
2. **Fund backups as a security control.** Given 95% of attacks target backups [22], require immutable or offline copies with separate credentials, and at least one full restore test of a tier-1 system each year.
3. **Treat supplier concentration as a board-level risk.** Require a register of tier-0/1 suppliers, an institution HHI (Section 8.3) and documented exit/fallback plans for any service scoring above 200 on exposure.
4. **Protect the responders.** Build wellbeing support, rota planning and external surge capacity into the incident plan [7][21].

13.2 For CIOs, CISOs and IT directors

Table 21. 90-day / 12-month roadmap

Metric	First 90 days	Within 12 months
Recovery time	Inventory tier-0/1 services; record current RTO/RPO; confirm backup isolation	Full restore rehearsal; measure actual vs RTO; close gaps >50%
Control coverage	Self-assess against CAF v4.0 / ECC-2:2024 / CERT-In audit scope; compute CCI	External audit or penetration test of tier-1 services; patch tier-1 within 14 days
Supplier concentration	Map services to suppliers and fourth parties; compute HHI	Renegotiate notification (≤24h), log access, data export and exit clauses for top-5 suppliers
Training uptake	Baseline click and report rates; privileged-user list	Quarterly simulations; 90%+ uptake; report rate above click rate
Service exposure	Score services (Table 15); check exposed assets and leaked credentials	Reduce exposure scores for top 3 services; peak-period fallback plans for LMS and SIS

13.3 For sector bodies, regulators and funders

- **UK:** Re-instate or expand awareness-testing measurement in sector guidance; consider whether shared HE platforms (LMS, SIS hosting) should be designated "critical suppliers" under the Cyber Security and Resilience Bill [52]; publish anonymised sector recovery-time benchmarks (Jisc).
- **Gulf:** Commission a recurring university cyber resilience survey modelled on the UK CSBS education annex; require branch campuses to document parent-campus dependencies and dual-jurisdiction notification plans.
- **India:** Establish an HE sectoral CSIRT or shared security service (on the CSIRT-Fin model [32]); publish university-level aggregates from CERT-In audits; provide DPDP compliance templates for colleges before 13 May 2027 [34]; add an exam-portal disruption scenario to CERT-In drills.

13.4 For suppliers serving higher education

- Commit to customer notification within 24 hours of confirmed compromise and provide customer-specific log extracts.
- Publish recovery architecture (multi-region, backup isolation) and support customer-run exit and restore tests.
- Harden support portals and free/trial account flows, the entry routes in the PowerSchool and Canvas incidents [17][54].

14. Tabletop exercise toolkit

A tabletop exercise offers a relatively low-risk way to test roles, decisions and the ability to maintain academic services without intrusive technical activity. The four scenarios are based on the kinds of incidents described in this report. Each is designed for a three-hour discussion involving institutional leadership, IT, legal and data protection, communications, registry and supplier management.

Table 22. Scenario library

Scenario	Based on	Key injects
A. LMS supplier breach in exam week	Canvas 2026 [12]	T+0 login pages show ransom message; T+2h supplier statement; T+6h students post screenshots; T+24h exam board must decide on deadlines; T+48h regulator query
B. Ransomware on student records	British Library 2023 [7]; Nottingham 2026 [10]	Encrypted SIS and backups attacked; data leak threat; payroll unaffected (cloud); OfS/ICO/CERT-In clocks start; UCAS/admissions deadline approaching
C. Identity/cloud outage (non-malicious)	CrowdStrike 2024 [18]	Mass device boot failure; SSO unavailable; manual workarounds; hands-on remediation of thousands of devices
D. File-transfer zero-day at a data intermediary	MOVEit 2023 [13]; Oracle EBS 2025 [14]	Supplier reveals student/alumni/finance data exfiltrated; institution has no logs; media enquiry; class-action risk

Table 23. Exercise scoring rubric (0–3 per criterion; maximum 30)

Criterion	Score 3 if…
1. Detection & escalation	Incident declared and severity set within 1 hour of first inject
2. Decision rights	Named decision-maker for shutdown, communications and ransom policy acted without delay
3. Regulatory clocks	All applicable notifications (e.g., CERT-In 6h; ICO/DPB 72h; OfS) identified with owners and times
4. Supplier engagement	Contract contacts, SLAs, notification and log-access rights located within 2 hours
5. Service prioritisation	Tier-0/1 restoration order agreed; RTOs referenced
6. Backup confidence	Team can state where clean backups are, who can access them and the last restore test date
7. Manual fallbacks	Documented workarounds for teaching, exams and payments activated
8. Communications	Holding statements for students, staff, partners and media approved within 4 hours
9. Wellbeing & capacity	Rota, external surge support and staff welfare addressed
10. Lessons capture	Actions logged with owners and deadlines; debrief scheduled

Score bands: 25–30 resilient; 18–24 developing; <18 at risk. Record scores per scenario to create a longitudinal recovery-readiness measure.

Annex A. Primary survey instrument

The survey below is designed to capture comparable institutional evidence without collecting credentials, exploitable weaknesses or other unnecessary sensitive detail. It should take approximately 25 minutes, with technical sections completed by the CIO/CISO or delegate and continuity questions checked by the responsible business owner. Response options are stated alongside each question.

Table A1. Survey items

ID	Question [response format]	Metric
P1	Country/emirate/state; institution type (public university, private university, college, branch campus); student FTE band [select]	Profile
P2	Is your institution a branch campus? If yes, which tier-0 services are provided by the parent institution? [multi-select list]	Supplier concentration
RT1	For each tier-0/1 service listed, state the approved RTO and RPO [hours; "none set"]	Recovery time
RT2	In the last 24 months, how many incidents caused loss of a tier-0/1 service for more than 4 hours? [number]	Recovery time
RT3	For the most disruptive incident: hours to containment, to minimum service and to full restoration [hours]	Recovery time
RT4	When did you last perform a full restore test of a tier-1 system from backup? [<6 months; 6–12; 12–24; never]	Recovery time
RT5	Are backups immutable or offline, with credentials separate from production identity? [yes / partly / no]	Recovery time
CC1	Which of these are in place? MFA (all staff / privileged only / none); patching within 14 days; EDR; 24x7 monitoring; network segmentation of tier-1; privileged access management [checklist]	Control coverage
CC2	Which framework do you assess against? [CAF / ECC / ISO 27001 / CIS / CERT-In audit / none]; date of last external assessment	Control coverage
CC3	Do you have a formal incident response plan, tested in the last 12 months? [plan + tested / plan only / none]	Control coverage
SC1	Number of suppliers providing tier-0/1 services [number]	Supplier concentration
SC2	Have you reviewed cyber risk for (a) immediate suppliers, (b) their key subcontractors? [yes / no for each]	Supplier concentration
SC3	For each tier-0/1 service, name the supplier category (not the brand if sensitive) [table]. Used to compute HHI	Supplier concentration
SC4	Do contracts with top-5 suppliers include: breach notification ≤24h; log access; data export; exit plan; right to audit? [checklist]	Supplier concentration
TU1	% of staff completing cyber training in last 12 months [%]	Training uptake
TU2	Latest simulated-phishing click rate and report rate [%; "not measured"]	Training uptake
TU3	Are students trained? [all / some programmes / none]	Training uptake
SE1	Number of internet-facing applications in your inventory [number band]	Service exposure
SE2	Do you monitor for leaked credentials of your domain? [yes / no]	Service exposure

ID	Question [response format]	Metric
SE3	Rate each tier-0/1 service on criticality, attack surface, supplier dependency and peak sensitivity [Table 15 scale]	Service exposure
RR1	FTE dedicated to cyber security; IR retainer in place? [number; yes/no]	Response resources
RR2	Cyber insurance [specific policy / within broader policy / none / don't know]	Response resources
RR3	Tabletop exercises in last 12 months, and whether any involved a supplier-failure scenario [number; yes/no]	Response resources

Sampling: stratify by region and institution type; target ≥ 30 institutions per region for descriptive statistics, with response-rate and non-response bias reported. Pilot with 3–5 institutions per region first.

Annex B. Authorised incident and recovery records protocol

1. **Authorisation:** Written data-sharing agreement signed by the institution's DPO/General Counsel; scope limited to incident metadata; right to withdraw.
2. **Fields requested:** incident ID (pseudonymised), category (ransomware, DDoS, supplier, outage, account compromise), services affected and tier, supplier involved (category), timestamps (detection, declaration, containment, minimum service, full restoration), notifications made and times, root-cause category, data affected (Y/N, categories only), lessons-learned status.
3. **Exclusions:** no personal data, no IP addresses, no vulnerability specifics, no attacker communications, nothing under legal privilege or active investigation.
4. **Processing:** compute recovery-time distributions (median, P90), RTO attainment ratio, and supplier-originated share; report only in aggregates of five or more institutions.
5. **Retention:** delete raw extracts after aggregation; keep the aggregated dataset with a documented audit trail.

Annex C. Non-intrusive control review checklist

This checklist supports a desk review of institutional policies, summaries and screenshots supplied with permission. It does not authorise scanning, penetration testing or access to live systems. Any broader assessment requires separate written approval and a defined security protocol.

Domain	Evidence requested
Governance	Board risk register entry; cyber reporting cadence; named accountable executive
Identity	MFA policy and coverage report; privileged account list (counts only); conditional-access summary
Backup & recovery	Backup architecture diagram; immutability settings; last restore-test record; RTO/RPO register
Suppliers	Supplier register for tier-0/1; sample contract clauses; supplier assurance questionnaires
Detection & response	IR plan; on-call rota; IR retainer; last two exercise reports
People	Training completion report; phishing simulation summary
Regulatory	Notification matrix (CERT-In, DPB, ICO, OfS, national CERTs); log retention settings (≥180 days India)

Annex D. Ethics, legal and data-licensing notes

- This report attributes publicly available statistics, analyses and public incident disclosures to their stated sources. Some UK government publications are made available under the Open Government Licence, subject to its terms; the licence applicable to each work should be checked. Third-party charts and material reproduced as images may require separate clearance.
- Before reproducing substantial third-party material, obtain a licence review and any permissions required by the relevant rights holder. Attribution alone is not a substitute for permission. The distribution rights for the underlying original report also need to be confirmed before public circulation.
- **Primary research** must follow applicable data protection law (UK GDPR, India DPDP Act, Saudi PDPL, UAE PDPL), institutional ethics approval where required, and the principle that no security-sensitive detail is published at institution level.
- **Named incidents** are drawn from public disclosures and reputable reporting; attacker claims are labelled as unverified.

Glossary

Term	Meaning
CCI	Control Coverage Index: mean adoption rate across a defined control set (this report)
CSBS	Cyber Security Breaches Survey (UK official statistics, DSIT/Home Office)
CSIRT	Computer Security Incident Response Team
DPB	Data Protection Board of India
ECC	Essential Cybersecurity Controls (Saudi National Cybersecurity Authority)
HHI	Herfindahl–Hirschman Index: sum of squared market or dependency shares (0–10,000)
IBC	International branch campus
LMS / VLE	Learning management system / virtual learning environment
RTO / RPO	Recovery time objective / recovery point objective
SIS	Student information (records) system
Tier-0 / Tier-1	Foundational / mission-critical services (Section 3.2)

Research limitations and interpretation

This study compares sources that differ in geography, sampling frame, definitions and observation period. UK official survey responses measure reported organisational controls and identified attacks; vendor telemetry measures detected attempts; ransomware surveys reflect respondents' experiences. These are not interchangeable measures, and the absence of published university-level evidence in the Gulf and India should not be mistaken for evidence of lower or higher resilience.

The Control Coverage Index is a derived measure of reported adoption, not a direct effectiveness audit. The service-tier objectives, exposure scores and supplier concentration examples are proposed analytical tools. Section 12 is based on an illustrative synthetic model, and the referenced underlying workbook was not supplied for independent reproduction. Its numerical associations must not be interpreted as empirical treatment effects or forecasts.

Information about incident events, legal duties and third-party market shares can change after the evidence cut-off. Users should consult the underlying source and, for legal requirements, the responsible regulator or qualified legal adviser. Outstanding verification and publication-rights matters are recorded separately in the internal Editorial Verification and Clearance Log.

References

The sources below are retained in the source report's numbered citation order. Entries have been formatted consistently where bibliographic detail is available. Principal findings were checked selectively against official primary publications during editorial review; this is not a claim that all 54 listed sources or every secondary figure were independently validated. Refer to the separate internal clearance log for outstanding checks.

#	Source
1	DSIT & Home Office (30 Apr 2026). Cyber security breaches survey 2025/2026: education institutions findings. Official statistics. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings
2	DSIT & Home Office (2025). Cyber security breaches survey 2025: education institutions findings. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-education-institutions-findings
3	Jisc (2026). Cyber attacks against UK education and research are growing more complex and sophisticated (news release on Cyber Threat Intelligence Report and Cyber Posture Survey). https://www.jisc.ac.uk/news/all/cyber-attacks-against-uk-education-and-research-are-growing-more-complex-and-sophisticated
4	Jisc (2026). Threat intelligence reveals increase in compromised credentials on the dark web. https://www.jisc.ac.uk/news/all/threat-intelligence-reveals-increase-in-compromised-credentials-on-the-dark-web
5	Jisc. Cyber security posture surveys (2022 results). https://jisc.ac.uk/reports/cyber-security-posture-surveys
6	NCSC (2025). NCSC Annual Review 2025 -Incident management. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-01-cyber-threat-to-the-uk/incident-management
7	British Library (8 Mar 2024). Learning lessons from the cyber-attack: British Library cyber incident review. https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf
8	Digital Health (Jun 2023). NHS patient data compromised in university cyber attack. https://www.digitalhealth.net/2023/06/nhs-patient-data-compromised-in-university-cyber-attack-report/
9	Computing (Apr 2024). Cyberattack disruption lingers at Cambridge University. https://www.computing.co.uk/news/4191482/cyberattack-disruption-lingers-cambridge-university
10	University of Nottingham (updated 20 Sep 2026). Cyber attack incident. https://www.nottingham.ac.uk/home/alerts/cyber-attack-incident.aspx
11	Inside Higher Ed (5 May 2026). "Pay or leak": hackers target big higher ed vendor. https://www.insidehighered.com/news/tech-innovation/administrative-tech/2026/05/05/pay-or-leak-hackers-target-big-higher-ed-vendor
12	Wikipedia (accessed Oct 2026). 2026 Canvas data breach (compiled timeline; cross-checked with [11]). https://en.wikipedia.org/wiki/2026_Canvas_data_breach
13	The Record (2023). MOVEit fallout continues: National Student Clearinghouse schools. https://therecord.media/moveit-fallout-continues-nsc-schools
14	The Register (2 Dec 2025). University of Pennsylvania joins list of victims from Clop's Oracle EBS raid. https://www.theregister.com/2025/12/02/clop_university_of_pennsylvania/
15	Infosecurity Magazine (Jul 2020). Blackbaud breach hits nine more universities. https://www.infosecurity-magazine.com/news/blackbaud-breach-hits-nine-more/
16	Imperial College London. USS -Capita cyber incident (staff information page). https://imperial.ac.uk/human-resources/pay-and-pensions/pensions/uss/capita-cyber-incident

#	Source
17	TechCrunch (7 Feb 2025). PowerSchool data breach affected 16,000 students in the UK. https://techcrunch.com/2025/02/07/powerschool-data-breach-affected-16000-students-in-the-uk
18	TechCrunch (20 Jul 2024). Microsoft says 8.5M Windows devices were affected by CrowdStrike outage. https://techcrunch.com/2024/07/20/microsoft-says-8.5m-windows-devices-were-affected-by-crowdstrike-outage
19	Synergy Research Group (2026). Q2 cloud market passes $143 billion; highest growth rate in eight years. https://www.srgresearch.com/articles/q2-cloud-market-passes-143-billion-highest-growth-rate-in-eight-years
20	Wikipedia (accessed Oct 2026). SITS:Vision (reported ~70% UK HE usage; secondary source). https://en.wikipedia.org/wiki/SITS:Vision
21	Sophos (Sep 2025). The State of Ransomware in Education 2025 (blog and press release). https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-education-2025
22	Sophos (2024). The State of Ransomware in Education 2024. https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-education-2024
23	SecurityBrief UK (2025). UK firms face rising ransomware costs but recover faster (Sophos State of Ransomware 2025). https://securitybrief.co.uk/story/uk-firms-face-rising-ransomware-costs-but-recover-faster
24	Security MEA (26 Jun 2025). Nearly half of companies in the UAE opt to pay the ransom (Sophos). https://securitymea.com/2025/06/26/nearly-half-of-companies-in-the-uae-opt-to-pay-the-ransom/
25	The Week / PTI (2 Jul 2025). Sophos: 53 pc of Indian firms surveyed paid ransom. https://www.theweek.in/wire-updates/business/2025/07/02/dcm40-biz-sophos-report.html
26	Help Net Security (23 Apr 2025). 2025 Data Breach Investigations Report: third-party breaches double. https://www.helpnetsecurity.com/2025/04/23/verizon-2025-data-breach-investigations-report-dbir/
27	KnowBe4 (13 May 2025). Security training reduces global phishing click rates by 86%. https://knowbe4.com/press/knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86
28	Check Point Research (2025). Cyber attacks surge against education sector ahead of back-to-school season. https://blog.checkpoint.com/research/cyber-attacks-surge-against-education-sector-ahead-of-back-to-school-season/
29	CXO Digital Pulse (22 Sep 2025). Indian education sector faces surge in cyberattacks, nearly double global average (Check Point Research). https://www.cxodigitalpulse.com/indian-education-sector-faces-surge-in-cyberattacks-nearly-double-global-average/
30	CRN Asia (Sep 2025). India sees 3,237 cyberattacks weekly per organisation (Check Point Research). https://www.crnasia.com/india/news-network/news/india-sees-3237-cyberattacks-weekly-per-organisation-education-and-government-among-the-top-targets-check-point-research
31	Careers360 (13 Aug 2025). Over 2 lakh cyberattacks, 4 lakh data breaches hit Indian educational institutions in 9 months (CyberPeace e-Kawach). https://news.careers360.com/over-2-lakh-cyberattacks-4-lakh-data-breaches-hit-indian-educational-institutions-in-9-months
32	Press Information Bureau, Government of India (Jan 2026). CERT-In year-end statistics document. https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/jan/doc2026123764501.pdf
33	Indian Computer Emergency Response Team (CERT-In) (28 April 2022). Directions under section 70B(6) of the Information Technology Act, 2000. Official directions and reporting obligations. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
34	Ministry of Electronics and Information Technology, Government of India (13–14 November 2025). Digital Personal Data Protection Rules, 2025, and commencement notification (G.S.R. 843(E)). https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025

#	Source
35	Lawrbit (2025). Comprehensive Cyber Security Audit Policy Guidelines (CERT-In, 25 Jul 2025). https://www.lawrbit.com/article/comprehensive-cyber-security-audit-policy-guidelines/
36	St Xavier's College Jaipur (24 Sep 2025). Notice regarding UGC Handbook on Cyber Hygiene 2025. https://sxcjpr.edu.in/wp-content/uploads/2025/09/Notice-regarding-UGC-Handbook-on-Cyber-Hygiene-2025.pdf
37	IBM India Newsroom (7 Aug 2025). India records highest average cost of a data breach at INR 220 million. https://in.newsroom.ibm.com/2025-08-07-India-Records-Highest-Average-Cost-of-a-Data-Breach-IBM
38	IBM MEA Newsroom (2025). Cost of a Data Breach 2025 -Middle East findings. https://mea.newsroom.ibm.com/codb-me-findings-2025
39	Gulf News (25 Feb 2025). UAE: 223,800 assets exposed to cyberattacks (UAE Cybersecurity Report 2025, CSC & CPX). https://gulfnews.com/uae/government/uae-223-800-assets-exposed-to-cyberattacks-as-ai-driven-attacks-rise-1.500046211
40	Khaleej Times (2026). 50% of cyberattacks in Gulf targeted UAE, Saudi Arabia in first half of 2026 (Positive Technologies). https://www.khaleejtimes.com/business/50-cyberattacks-uae-saudi-arabia-first-half-2026-report
41	AGBI (Aug 2026). UAE thwarts cyberattacks on aviation, energy and education. https://www.agbi.com/cybersecurity/2026/08/uae-thwarts-cyberattacks-on-aviation-energy-and-education/
42	Secure.com (2025). Saudi businesses: NCA ECC update (ECC-2:2024). https://www.secure.com/blog/compliance/saudi-businesses-nca-ecc-update
43	Telecom Review (2024). From role models to evolving players: Arab states in the ITU GCI 2024. https://static.telecomreview.com/articles/reports-and-coverage/8392-from-role-models-to-evolving-players-assessing-arab-states-in-the-itu-s-gci-2024
44	DT Next (Sep 2024). India jumps to Tier 1 in Global Cybersecurity Index 2024. https://www.dtnext.in/news/business/india-jumps-to-tier-1-in-global-cybersecurity-index-2024-803536
45	Education-UAE (2025). Dubai higher education growth 2025 (KHDA data). https://www.education-uae.com/dubai-higher-education-growth-2025/
46	Wikipedia (accessed Oct 2026). Higher education in Saudi Arabia. https://en.wikipedia.org/wiki/Higher_education_in_Saudi_Arabia
47	Vikaspedia / Ministry of Education (2024). AISHE 2021-22 release. https://vikaspedia.in/news/ministry-of-education-releases-all-india-survey-on-higher-education-2021-2022
48	Ministry of Education, Government of India (8 July 2026). Ministry releases All India Survey on Higher Education (AISHE) reports for 2022–23 and 2023–24. Press Information Bureau (PRID 2282525). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2282525
49	ACA Secretariat (2026). HESA publishes first release of 2024/25 UK student data. https://aca-secretariat.be/newsletter/hesa-publishes-first-release-of-2024-25-uk-student-data/
50	The PIE News (14 May 2026). OfS: English universities warned of over-optimism as a third face deficits. https://thepienews.com/ofs-english-universities-warned-of-over-optimism-as-a-third-face-deficits/
51	teiss (Jul 2025). UK cracks down on ransomware payments with new public sector ban. https://www.teiss.co.uk/news/uk-cracks-down-on-ransomware-payments-with-new-public-sector-ban-16124
52	Mayer Brown (Nov 2025). Cyber Security and Resilience (Network and Information Systems) Bill introduced to Parliament. https://www.mayerbrown.com/ja/insights/publications/2025/11/cyber-security-and-resilience-network-and-information-systems-bill--introduced-to-parliament

#	Source
53	NCC Group (Aug 2025). Introducing the Cyber Assessment Framework 4.0. https://www.nccgroup.com/introducing-the-cyber-assessment-framework-4-an-updated-tool-for-uk-cyber-resilience/
54	Bushido Token (May 2026). UK Cybercrime Journal: British universities struck by ShinyHunters before exam season. https://blog.bushidotoken.net/2026/05/uk-cybercrime-journal-british.html
55	U.S. Department of Education, Federal Student Aid (12 May 2026; updated 29 May 2026). Technology Security Alert: Ongoing Cybersecurity Incident Involving the Canvas Learning Management System. https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2026-05-12/technology-security-alert-ongoing-cybersecurity-incident-involving-canvas-learning-management-system-updated-may-29-2026
56	U.S. House Committee on Homeland Security (11 May 2026). Letter to Instructure Holdings concerning Canvas cybersecurity incidents. https://homeland.house.gov/wp-content/uploads/2026/05/2026.05.11-Homeland-to-Instructure-Holdings-Inc.pdf

Commissioned consultancy reports

A sector-level report can identify common exposures and useful measures, but each institution's systems, service arrangements, regulatory duties and risk appetite are different. Institution-specific findings therefore require authorised primary records, consent and a clearly defined assessment scope.

> Institution-specific research
> The five-measure framework, evidence-request protocol and exercise rubric can provide the basis for a separately commissioned institutional study. Such work should be undertaken only with agreed scope, written authority and appropriate confidentiality and data-protection arrangements.

Publication enquiries: EQSC Global.

© 2026 EQSC Global. Third-party research and source material remain subject to their respective rights and licences (Refer to the Disclaimer and Notice on the opening page of this document). Figures in Section 12 are synthetic and illustrative, not results of a field survey. This report does not constitute legal, regulatory or financial advice.

This page has been intentionally kept blank.

The Questions are Yours.
The Discovery is Ours.

This report is a glimpse of the investigative research, evidence-led analysis and strategic intelligence EQSC Global can deliver. Every institution and organisation faces questions that deserve more than assumptions.

Commission a bespoke study with EQSC Global to uncover the evidence, reveal opportunities and find the answers that matter to your next big decision.

Your Question. Our Research. Your Answer

EQSC

eqscglobal.com/commissioned-research

The Path Forward

The choices higher education leaders make today will define the academic landscape for decades to come. Navigating shifting demographics, economic pressures, and technological disruption requires more than just adaptation - it demands rigorous foresight.

Our report transforms complex institutional data into strategic clarity, providing global universities with the empirical foundation needed to secure institutional sustainability, elevate academic excellence, and inspire the next generation of learners.

Commissioned Report | Executive Intelligence & Advisory

EQSC

eqscglobal.com

EQSC

eqscglobal.com